VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA EKONOMICKÁ FAKULTA

KATEDRA APLIKOVANÉ INFORMATIKY

Audit a testování bezpečnosti informací v malých firmách

Audit and Testing Information Security in Small Companies

Student: Bc. Michal Blaško

Vedoucí diplomové práce: Ing. Jan Ministr, Ph.D.

Ostrava 2014

VŠB - Technická univerzita Ostrava
Ekonomická fakulta
Katedra aplikované informatiky

Zadání diplomové práce

Student: **Bc. Michal Blaško**

Studijní program: N6209 Systémové inženýrství a informatika

Studijní obor: 1802T001 Aplikovaná informatika

Téma: Audit a testování bezpečnosti informací v malých firmách
Audit and Testing Information Security in Small Companies

Zásady pro vypracování:

1. Úvod
2. Teoretická a metodická východiska řízení bezpečnosti informací
3. Analýza stávajícího stavu ve firmě
4. Návrh inovace bezpečnosti
5. Závěr

Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků diplomové práce
Seznam příloh
Přílohy

Seznam doporučené odborné literatury:

DOUCEK, Petr et al. *Řízení bezpečnosti informací.* 2. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.
CALDER, Alan and Steve WATKINS. *IT Governance: An International Guide to Data Security and ISO27001/ISO27002.* 5th ed. London: Kogan page, 2012. ISBN 978-0-7494-6485-1.
CAZEMIER, J. A., P. L. OVERBEEK and L. M. C. PETERS. *Security Management.* London: The Stationery Office, 2006. ISBN 0-11-330014-X.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Jan Ministr, Ph.D.**

Datum zadání: 22.11.2013
Datum odevzdání: 25.04.2014

Ing. Petr Rozehnal, Ph.D.
vedoucí katedry

prof. Dr. Ing. Dana Dluhošová
děkanka fakulty

Prohlašuji, že jsem celou práci, včetně všech příloh, vypracoval samostatně.

Datum odevzdání: 25. dubna 2014 Podpis: ……

Obsah

1 Úvod 5

2 Teoretická a metodická východiska řízení bezpečnosti informací 7

2.1 Legislativa a normy bezpečnostního auditu IT 7

2.2 Mezinárodní normy pro řízení bezpečnosti informací 7

2.2.1 Normy pro návrh 8

2.2.2 Normy pro kontrolu 13

2.2.3 Legislativa 22

2.3 Metodika bezpečného IS ve společnosti – Systém managementu informační bezpečnosti PDCA 22

2.3.1 Plan – plánuj 23

2.3.2 Do – dělej 27

2.3.3 Check – kontroluj 31

2.3.4 Act – jednej 34

2.4 Principy provádění bezpečnostního auditu 37

3 Analýza stávajícího stavu ve firmě 40

3.1 Charakteristika stávajícího stavu firmy 40

3.2 Analýza rizik 44

3.2.1 Identifikace aktiv 44

3.2.2 Ohodnocení aktiv 45

3.2.3 Identifikace hrozeb 46

3.2.4 Frekvence výskytu bezpečnostních incidentů a jejich dopady 46

3.2.5 Určení zranitelnosti jednotlivých bezpečnostních hrozeb 47

3.2.6 Základ pro určení kritických míst 48

4 Návrh inovace bezpečnosti 50

4.1 Vyhodnocení aktiv 50

4.2 Návrhy a doporučení 51

4.3 Rekapitulace závěrů 52

5 Závěr 54

Seznam použité literatury

Seznam zkratek a pojmů

Prohlášení o využití výsledků diplomové práce

1 Úvod

V dnešním digitálním věku, kde žijeme a pracujeme, občané a podniky hledají informační a komunikační technologie (ICT) neocenitelné pro provádění každodenních úkolů. Zároveň mají podniky i občané čím dál tím větší pravděpodobnost narušení bezpečnosti. To je díky chybám v těchto nových i stávajících technologiích, spolu s korektorem konvergence, k významnému nárůstu "stálého"' spojení a průběžného a exponenciálního uživatelského zavádění v členských státech.

Takové narušení bezpečnosti může být IT, například prostřednictvím počítačových virů nebo jiným škodlivým softwarem, systém selhání nebo poškození dat, nebo může být společensky motivováno, například prostřednictvím krádeže majetku nebo jiných mimořádných událostí způsobených zaměstnanci. Ve věku stále více závislém na digitální informaci, je zvyšující se počet nebezpečí. Hrozbou také je, že značný počet koncových uživatelů si neuvědomuje, jejich náchylnost k bezpečnostním rizikům. Vzhledem k rostoucí úrovni porušení, je mnohem důležitější než kdy jindy, aby organizace zvyšovaly povědomí o bezpečnosti tím, že nasměrují uživatele do první linie obrany.

Bezpečnostní prostředí se neustále mění. S rozvojem a šířením bezpečnostních hrozeb, bude řešení informační bezpečnosti, které je používáno dnes, již zítra zastaralé. Zabránit těmto hrozbám lze soustavnou prevencí, která je však dnes často velmi podceňována. Efektivním nástrojem pro poznání stavu informační bezpečnosti a jejího řízení je bezpečnostní audit ICT.

Tato práce se zabývá bezpečnostním auditem, mapuje normy a způsoby nasazení a ukazuje na konkrétním příkladě, jak muže takový audit vypadat, jak probíhá a co přináší.

Jako model pro moji práci posloužila firma Fashion Arena Outlet Centrum (FAOC), s. r.o., konkrétně na jejich oddělení Fashion Arena Center Management, která působí v oblasti obchodování a je největší outletové centrum v České republice.

Teoretická část práce čerpá z nejrůznějších zdrojů a podává souhrnný přehled o hlavním proudu toho, co se obecně považuje za bezpečnostní auditing IT. Také předkládá a poskytuje detailní informace týkající se legislativy mezinárodně uznávaných norem

pro řízení bezpečnosti informací a blíže popisuje metodiku budování bezpečného IS ve společnosti.

Druhá část práce se věnuje analýze výchozího stavu infrastruktury informačních technologií ve firmě. To znamená audit hardwarového a softwarového vybavení, jejich nastavení, poskytovaných služeb a architektury sítě. V této části práce byly taktéž identifikovány objekty, které jsou pro firmu cenné a které je důležité zabezpečit.

Hlavním cílem třetí části práce již byly návrhy ke snížení rizik.

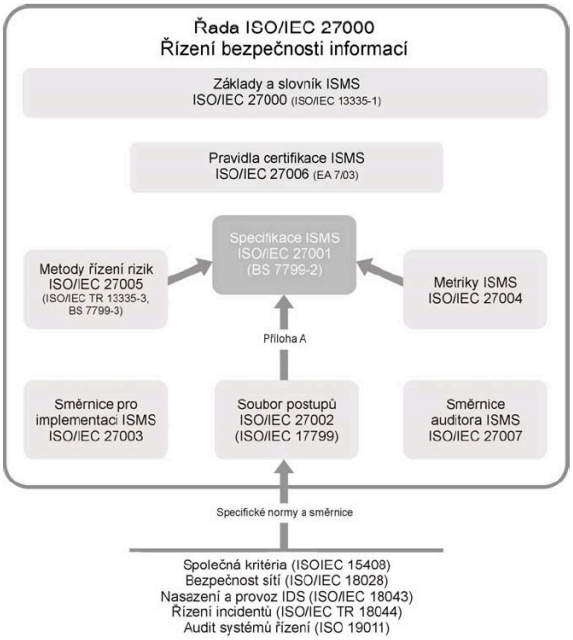
2 Teoretická a metodická východiska řízení bezpečnosti informací

2.1 Legislativa a normy bezpečnostního auditu IT

V dnešní vysoce vyspělé době informačních technologií již není možné se při auditu těchto vysoce sofistikovaných informačních systémů spoléhat pouze na vlastní zkušenosti a zkušenosti pracovníků v organizaci působící. Dále pak s ohledem na integraci ČR do evropské unie je třeba se přizpůsobit evropským trendům a přijmout pravidla tohoto společenství za vlastní. Z tohoto důvodu byla ve spolupráci s evropskými normalizačními institucemi vyvinuta rodina norem a legislativ, dle které by se měl každý subjekt, který tento audit informačních technologií realizuje, řídit. V neposlední řadě slouží tyto normy jako metrika, která zaručuje srovnatelnost a transparentnost s audity prováděnými v jiných společnostech a také mezi auditorskými autoritami navzájem.

2.2 Mezinárodní normy pro řízení bezpečnosti informací

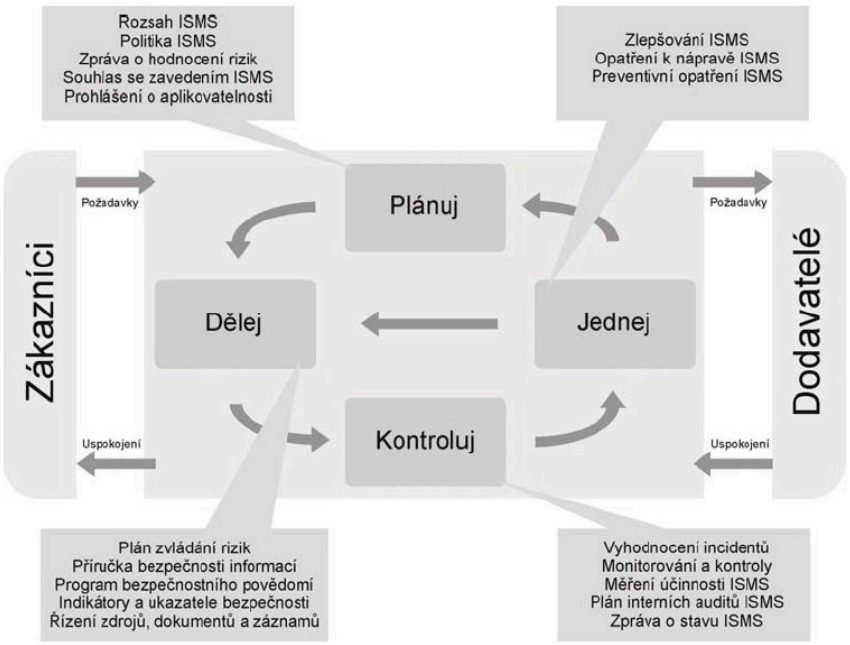
Na jaře roku 2005 organizace ISO (International Organization for Standardization) ohlásila zavedení nové série norem ISO/IEC 27000. ISO rezervovala sérii ISO 27000 pro normy z oblasti bezpečnosti informací.



Obrázek 1: Koncept řady ISO/IEC 27000

Nová řada norem pro řízení bezpečnosti informací ISO/IEC 27000 vychází ideově z konceptu PDCA a jejím základem jsou normy, jež jsou uvedeny na obrázku číslo 1.

Podobně jako u jiných systémů řízení (např. ISO 9001, ISO 14001) je za jádro normalizace považována definice systému. V případě ISMS se tak stává klíčovým prvkem mezinárodní norma **ISO/IEC 27001:2005 – Information security management system – Requirements** (Systém řízení bezpečnosti informací – Požadavky), která vychází ze známého britského standardu BS 7799-2 a která byla vydána v říjnu roku 2005. Nosné prvky, které norma vyžaduje pro budování ISMS, jsou vidět na následujícím obrázku. [1]



Obrázek 2: PDCA Model pro bezpečnost informací

2.2.1 Normy pro návrh

ISO/IEC 27002 (dříve BS 17799) - Code of praktice for information security management

ISO/IEC 27002:2013 je sbírka nejlepších bezpečnostních praktik a může být využita jako kontrolní seznam všeho správného, co je nutno pro bezpečnost informací v organizaci udělat. Aktuální verze normy "ISO/IEC 27002:2013 Information technology - Security

techniques - Code of practice for information security management" je mezinárodně přijatý standard, sbírka nejlepších praktik z oblasti bezpečnosti informací.

35 cílů opatření

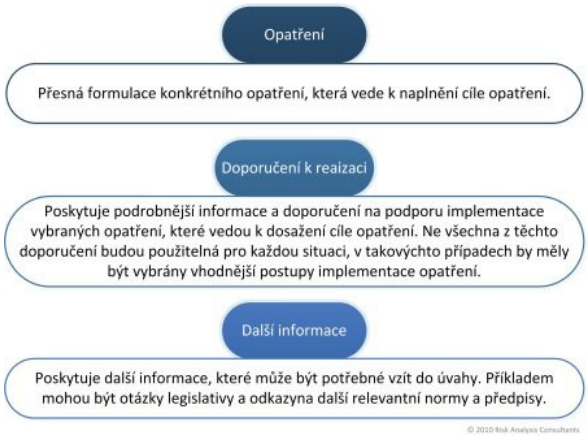
14 hlavních oddílů ISO/IEC 27002:2013 definuje 35 cílů (kontrolních) opatření pro ochranu informačních aktiv proti narušení jejich důvěrnosti, dostupnosti a integrity. V podstatě tyto cíle opatření zahrnují funkční požadavky pro architekturu bezpečnosti informací organizace.

Cíle opatření poskytují kvalitní základ pro definici sady "axiomů" pro bezpečnostní politiku. Ne všechny jsou aplikovatelné v každé organizaci a mohou se objevit požadavky na jejich přeformulování či přizpůsobení podle aktuálních potřeb organizace. Nicméně většina z nich je obecně použitelná.

100vky specifických opatření

ISO/IEC 27002 také popisuje nejlepší praktiky pro zajištění bezpečnosti informací, které by organizace měla vzít úvahu pro zajištění kontrolních cílů. Nová verze normy obsahuje 114 "základních" opatření (v předchozí verzi normy z roku 2005 to bylo 133), které se, ale ve skutečnosti dále rozpadají na stovky specifických bezpečnostních opatření.

Popis opatření je strukturován následovně:



Obrázek 3: Popis opatření

Norma nepřikazuje, která opatření musí být bezpodmínečně aplikována, ale ponechává rozhodnutí na organizaci. Vhodná opatření jsou vybírána na základě hodnocení rizik a jejich

implementace je závislá na konkrétní situaci. Cílem není implementovat vše, co norma popisuje, ale spíše naplnit všechny aplikovatelné cíle opatření. Tento přístup zajišťuje, že norma je široce aplikovatelná a dává uživatelům velkou flexibilitu při implementaci. Nicméně toto přináší obtíže při certifikaci, kdy může být složité posoudit, zda jsou aktuální bezpečnostní opatření plně v souladu s normou. Navíc certifikace se týká zavedení **ISMS** a organizace je tak certifikována podle ISO/IEC 27001, které obsahuje shrnutí opatření z ISO/IEC 27002 vedle procesů k hodnocení rizik a výběru bezpečnostních opatření. [7]

Následují další standardy z rodiny 27000 – dále specifikující ISMS. Normy jsou založené na bázi modelu PDCA (Plan, Do, Check, Act). Návrh ISMS -> Implementace ISMS -> Monitorování a kritické hodnocení ISMS -> Vylepšení a korekce ISMS -> Návrh ISMS…. Tento model bude podrobně popsán dále (a je například také bází standardu kvality ISO 9001).

ISO/IEC 27003 - Information security management system implementation guidance

ISO/IEC 27003 byla oficiálně publikována v únoru roku 2010. Norma obsahuje především **návod k implementaci** ostatních norem série 27000 a je určena k využití ve všech typech organizací, které mají v úmyslu zavést systém řízení bezpečnosti informací (ISMS) dle ISO/IEC 27001. [8]

ISO/IEC 27004 Information security management metrics and measurement

ISO/IEC 27004 je pro organizace pomůckou k měření a prezentaci efektivity jejich systémů řízení bezpečnosti informací (ISMS), zahrnující řídící procesy definované v ISO/IEC 27001 a opatření z ISO/IEC 27002. Norma byla publikována v prosinci roku 2009.

Tato norma je pro organizace pomůckou k měření a prezentaci efektivity jejich systémů řízení bezpečnosti informací (ISMS) zahrnující řídící procesy definované v ISO/IEC 27001 a opatření z ISO/IEC 27002. [9]

ISO/IEC 27005 - Information Security Risk Management

SO/IEC 27005:2011 poskytuje doporučení a techniky pro analýzy informačních rizik. Jejím základem jsou revize dříve vydaných norem ISO/IEC TR 13335-3:1998, ISO/IEC TR 13335-4:2000 a využití některých pasáží BS 7799-3.

Norma obsahuje doporučení pro řízení rizik bezpečnosti informací s ohledem na požadavky ISMS dle ISO/IEC 27001:2005.

Mezi činnosti řízení rizik, které jsou definovány normou, patří:

Stanovení kontextu - vymezení základních kritérií pro řízení bezpečnosti informací, definice rozsahu a hranic, a stanovení organizační struktury pro řízení rizik.

Hodnocení rizik - identifikace rizik, kvantifikace nebo kvalitativní popis rizik a prioritizace rizik v souladu s kritérii a cíly hodnocení rizik.

Zvládání rizik - výběr protiopatření k redukci, podstoupení, vyvarování se nebo přenosu rizik a definice plánu zvládání rizik.

Akceptace rizik - učinění a formální zaznamenání rozhodnutí akceptace rizika a odpovědností za tato rozhodnutí

Seznámení s riziky - výměna a/nebo sdílení informací o rizicích

Monitorování a přezkoumávání rizik - monitorování a přezkoumávání rizik a jejich faktorů

První verze normy vyšla v roce 2008. Druhá, poslední verze byla vydána v červnu 2011. [10]

ISO/IEC 13335 - Management of information and communications technology security

Tato norma je českou verzí mezinárodní normy ISO/IEC TR 13335-3:1998. Mezinárodní norma ISO/IEC TR 13335-3:1998 má status české technické normy. ISO/IEC TR 13335 se skládá z následujících částí: Část 1: Pojetí a modely bezpečnosti IT, Část 2:

Řízení a plánování bezpečnosti IT, Část 3: Techniky pro řízení bezpečnosti IT, Část 4: Výběr ochranných opatření a Část 5: Ochranná opatření pro externí spojení. Tato třetí část (ČSN) ISO/IEC TR 13335 se zabývá technikami pro řízení bezpečnosti IT. Techniky jsou založeny na obecných směrnicích uvedených v ISO/IEC TR 13335-1 (v ČR zavedena jako ČSN ISO/IEC 13335-1) a ISO/IEC TR 13335-2 (v ČR zavedena jako ČSN ISO/IEC 13335-2). Tyto směrnice byly navrženy s cílem usnadnit implementaci bezpečnosti IT. Tyto směrnice jsou užitečné pro identifikaci a řízení všech aspektů bezpečnosti IT. Pro úplné pochopení této části je nutné pochopení pojetí a modelů zavedených v části 1 a nástrojů, týkajících se řízení a plánování bezpečnosti IT, popsaných v (ČSN) ISO/IEC TR 13335-2. [5]

ISO/IEC TR 15945 - Specification of TTP services to support the aplication of digital signatures

Tato norma je českou verzí mezinárodní normy ISO/IEC 15945:2002. Mezinárodní norma ISO/IEC 15945:2002 má status české technické normy. Slouží jako specifikace služeb TTP na podporu aplikace digitálních podpisů. [4]

ISO/IEC TR 18043 - System deployment a operations of intrusion detection systems - IDS

Technická zpráva s metodickým návodem jak zahrnout IDS do IT struktury.

ISO/IEC 27035:11 (dříve ISO/IEC TR 18044) - Information security incident management

Norma přepracovává a nahrazuje původní ISO/IEC TR 18044 z roku 2004. *ISO/IEC 27035:2011* je zaměřena na řízení incidentů bezpečnosti informací. Věnuje se postupům včasné detekce incidentů, jejich hlášení, vyhodnocení závažnosti a následné reakce. Dává doporučení pro identifikaci existujících zranitelností, posouzení jejich závažnosti a přijetí odpovídajících preventivních a nápravných opatření. [11]

Dále ISO/IEC specifikuje radu kryptografických a autentizačních technik a mechanismu například v normách: **ISO/IEC 9796**, **ISO/IEC 9797**, **ISO/IEC 9798**, **ISO/IEC 10116**, **ISO/IEC 10118**, **ISO/IEC 11770**, **ISO/IEC 13888**, **ISO/IEC 14888.**

2.2.2 Normy pro kontrolu

Nyní byla představena fáze, kdy byl vytvořen bezpečný informační systém, to znamená, že v našem IS je provozován ISMS jako proces. Jak zákazníkům či partnerům v případě potřeby prokázat tuto vlastnost našeho systému? Případně si je třeba představit situaci, že stojíme před úkolem otestovat IS v jiné organizaci a určit, zda je bezpečný. I v takovém případě je možné postupovat dle známých a osvědčených pravidel, která jsou specifikována v mezinárodně uznávaných normách.

Jedním ze standardu, který lze použít na audit bezpečnosti IT je norma

ISO/IEC 15408

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém světové normalizace. Národní orgány, které jsou členy ISO a IEC, se podílejí na vývoji mezinárodních norem prostřednictvím technických komisí, zřízených příslušnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují i mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk.

Mezinárodní normy jsou navrhovány v souladu s pravidly uvedenými v části 3 direktiv ISO/IEC.

ISO a IEC ustavily v oblasti informačních technologií společnou technickou komisi, ISO/IEC JTC 1. Návrhy mezinárodních norem, přijaté společnou technickou komisí, se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících členů.

Mezinárodní norma ISO/IEC 15408-1 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie,* ve spolupráci s Organizacemi sponzorujícími projekt Společná kritéria. Identický text ISO/IEC 15408-1 je zveřejněn Organizacemi sponzorujícími projekt Společná kritéria pod názvem *Společná kritéria pro hodnocení bezpečnosti informačních technologií*. V příloze A ISO/IEC 15408-1 jsou uvedeny další informace o projektu Společná kritéria a kontaktní informace na Organizace sponzorující projekt.

ISO/IEC 15408 se skládá z následujících částí se společným názvem *Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT:*

- ***Část 1: Úvod a všeobecný model***
- ***Část 2: Bezpečnostní funkční požadavky***
- ***Část 3: Požadavky na zaručitelnost bezpečnosti***

ISO/IEC 15408, norma o více částech, vymezuje kritéria, která jsou zde z historických důvodů a pro zachování kontinuity uváděna jako Common Criteria (CC), která mají být použita jako základ pro hodnocení bezpečnostních vlastností produktů a systémů IT. Ustavením takové základny Společných kritérií budou mít výsledky hodnocení bezpečnosti IT význam pro širší veřejnost.

CC umožní srovnatelnost výsledků nezávislých hodnocení bezpečnosti. Provádějí to poskytnutím obecné množiny požadavků na bezpečnostní funkce produktů a systémů IT a na opatření týkající se záruk, která jsou aplikovaná v průběhu hodnocení bezpečnosti. Proces hodnocení ustavuje určitý stupeň důvěry, že bezpečnostní funkce takových produktů a systémů a na ně aplikovaná opatření týkající se záruk splňují tyto požadavky. Výsledky hodnocení mohou pomoci spotřebitelům určit, zdali je produkt nebo systém IT dostatečně bezpečný pro jejich zamýšlenou aplikaci a zdali je možné tolerovat bezpečnostní rizika implicitně vyplývající z jejich používání.

CC jsou užitečná jako návod pro vývoj produktů nebo systémů s bezpečnostními funkcemi IT a pro pořizování komerčních produktů a systémů s takovými funkcemi. V průběhu hodnocení je takový produkt nebo systém IT nazýván předmět hodnocení (TOE). Předmět hodnocení (TOE) zahrnuje například operační systémy, počítačové sítě, distribuované systémy a aplikace.

CC se zabývají ochranou informací před neautorizovaným zpřístupněním, změnou nebo ztrátou možnosti jejich použití. Kategorie ochrany vztahující se k těmto třem typům selhání bezpečnosti jsou obecně označovány jako důvěrnost, integrita a dostupnost. CC je možné aplikovat rovněž na další aspekty bezpečnosti. CC se soustřeďují na hrozby vůči informacím, které jsou výsledkem lidských aktivit, ať už škodlivých nebo jiných, ale mohou být

aplikovatelná právě tak na některé hrozby, které nesouvisí s lidskou činností. CC mohou být kromě toho aplikována v dalších oblastech IT, nečiní si však nárok na kompetentnost mimo oblast bezpečnosti IT.

CC jsou aplikovatelná na IT bezpečnostní opatření implementovaná v hardwaru, firmwaru nebo softwaru. Bude-li záměrem aplikovat specifické aspekty hodnocení pouze na určité metody implementace, bude to vyznačeno v relevantních tvrzeních kritérií.

Určitá témata, protože zahrnují specializované techniky nebo protože jsou vzhledem k bezpečnosti IT poněkud okrajová, jsou považována za témata, přesahující rámec CC. Některá z nich jsou uvedena dále.

a) CC neobsahují kritéria pro hodnocení bezpečnosti týkající se administrativních bezpečnostních opatření, která nesouvisí přímo s IT bezpečnostními opatřeními. Často však může být významná část bezpečnosti TOE dosažena pomocí administrativních opatření jako jsou organizační, personální, fyzické a procedurální kontroly. Administrativní bezpečnostní opatření v provozním prostředí TOE jsou považována za předpoklad bezpečného použití, kdy tato opatření mají dopad na schopnost IT bezpečnostních opatření čelit identifikovaným hrozbám.

b) Hodnocení technicko-fyzických aspektů bezpečnosti IT, jako je kontrola elektromagnetického vyzařování, není specificky řešena, i když mnoho z uplatněných pojmů je možné na tuto oblast aplikovat. CC řeší zejména některé aspekty fyzické ochrany TOE.

c) CC se nezabývá metodologií hodnocení ani administrativním a právním rámcem, na základě kterého mohou být kritéria aplikována hodnotícími autoritami. Očekává se však, že CC budou použita pro účely hodnocení v kontextu takového rámce a takové metodologie.

d) Postupy pro použití výsledků hodnocení při akreditaci produktu nebo systému jsou mimo rámec CC. Akreditace produktu nebo systému je administrativní proces, kterým je uděleno oprávnění provozovat produkt nebo systém IT v jeho plném provozním prostředí. Hodnocení je zaměřeno na IT bezpečnostní části produktu nebo systému a na ty části provozního prostředí, které mohou přímo ovlivnit bezpečné používání prvků IT. Výsledky procesu hodnocení jsou následně cenným vstupem pro akreditační proces. Protože však pro posouzení bezpečnostních vlastností produktů nebo systémů nesouvisících s IT a jejich vztahu

k bezpečnostním částem IT jsou vhodnější jiné techniky, měli by akreditační činitelé přijmout v případě takových aspektů jiná opatření.

e) CC se nezabývají předmětem kritérií pro hodnocení inherentních kvalit kryptografických algoritmů. V případě, že by bylo požadováno nezávislé hodnocení matematických vlastností kryptografie, obsažené v TOE, schéma hodnocení, na základě kterého jsou CC aplikována, musí zajistit pro taková hodnocení příslušné opatření. [3]

Srovnatelnou metodikou je projekt amerického ministerstva obrany, který vznikl v roce 1985 kvůli hodnocení operačních systému pro použití v armádních instalacích.

Trusted Computer System Evaluation Criteria (TCSEC) neboli kritéria hodnocení spolehlivosti počítačových systémů je normou ministerstva obrany vlády Spojených států amerických (DoD – Department of Defense), která stanoví základní požadavky pro hodnocení kontroly efektivnosti počítačové bezpečnosti v počítačovém systému. TCSEC byla využita pro hodnocení, klasifikaci a výběru počítačových systémů, u kterých bylo zvažováno jejich využití pro zpracování, ukládání a vyhledávání citlivých nebo tajných informací.

TCSEC, o které se často mluví jako o Oranžové knize, je ústředním bodem publikací Duhové řady ministerstva obrany Spojených států amerických. Původně byla vydána v roce 1983 Národním počítačovým bezpečnostním centrem (National Computer Security Center – NCSC), částí Národní bezpečnostní agentury (National Security Agency - NSA) a byla doplněna v roce 1985. TCSEC byla nahrazena Common Criteria, mezinárodním standardem, který byl vydán v roce 2005.

Základní cíle a požadavky

Politika:

Bezpečnostní politika musí být výslovná, dobře definovaná a v počítačovém systému vymahatelná. Existují dvě základní bezpečnostní politiky:

povinná bezpečnostní politika – Prosazuje pravidla řízení přístupu založené přímo na oprávnění jednotlivců, autorizaci pro informace a žádá utajení určité úrovně informací. Dalšími nepřímými faktory jsou faktory fyzické a týkající se okolí. Tato politika musí také

přesně odrážet zákony, obecné zásady a další relevantní pokyny, ze kterých jsou pravidla odvozena.

volná bezpečnostní politika – Prosazuje konzistentní sadu pravidel pro kontrolu a omezený přístup založený na základě určených osob, u kterých je stanoveno, že určité informace potřebují vědět.

Zodpovědnost:

Bez ohledu na politiku musí být prosazena osobní zodpovědnost. Musí existovat bezpečný způsob, který by zajistil přístup oprávněného, příslušného zástupce, který dokáže vyhodnotit zodpovědnost k informacím v přiměřeném čase a bez zbytečných potíží. Jsou tři požadavky vyplývající z cíle zodpovědnosti:

identifikace – proces k rozpoznání jednotlivých uživatelů,

autentifikace – ověření oprávnění uživatelů pro konkrétní kategorie informací,

audit – informace z auditu musí být drženy a chráněny tak, aby akce zasahující do bezpečnosti mohly být vystopovány k autentifikovanému jednotlivci.

Záruka:

Počítačový systém musí obsahovat hardwarové nebo softwarové mechanismy, které mohou být nezávisle hodnoceny k poskytnutí dostatečné záruky, že systém splňuje výše uvedené požadavky. Obecněji řečeno musí záruka obsahovat ujištění, že důvěrné části systémové fungují tak, jak bylo zamýšleno. Ke splnění těchto cílů je třeba dvou typů záruky s těmito jejich částmi:

- **záruční mechanismy**
- **provozní záruka** – systémová architektura, systémová integrita, skryté využívání kanálů, analýza, spolehlivý facility management a důvěryhodné ozdravení,
- **záruka v průběhu životního cyklu** – testování bezpečnosti, navrhované specifikace a verifikace, uspořádané řízení a důvěryhodná distribuce systému,
- **záruka nepřetržité ochrany** – Důvěryhodné mechanismy, které prosazují tyto základní požadavky, musí být nepřetržitě chráněny proti manipulacím a/nebo neoprávněným změnám.

Dokumentace:

V každé třídě je další sada dokumentace, která řeší spíše vývoj, implementaci a správu systému než jeho schopnosti. Tato dokumentace zahrnuje:

- uživatelský návod k bezpečnostnímu programu, manuál k zařízení, testovací dokumentaci a projektovou dokumentaci.

Divize a třídy

TCSEC definuje čtyři divize: D, C, B a A, kdy A znamená největší bezpečnost. Každá divize znamená důležitý rozdíl v důvěře, kterou může člověk či organizace věnovat vyhodnocenému systému. C, B a A jsou navíc rozděleny do několika hierarchických oddělení, do tzv. tříd C1, C2, B1, B2, B3 a A1.

Každá divize a třída rozšiřuje nebo mění dané požadavky, které od sebe odlišují jednotlivé divize nebo třídy.

D – minimální ochrana

Určeno pro systémy, které byly vyhodnoceny, ale nesplňují požadavky pro zařazení do vyšší divize.

C – volitelná ochrana

C1 – volitelná bezpečnostní ochrana

- identifikace a autentizace
- oddělení uživatelů a dat
- řízení přístupu schopné prosadit omezení přístupu a individuální princip fungování
- požadovaná systémová dokumentace a uživatelský návod

C2 – kontrolovaná ochrana přístupu

- jemněji definované řízení přístupu
- individuální zodpovědnost díky přihlašovacím procedurám
- sledování auditem
- opětovné užití

- izolace zdrojů

B – povinná ochrana

B1 – ochrana bezpečnosti návěštím

- neformální vyhlášení bezpečnostní politiky
- značení bezpečnostní citlivosti dat
- povinná přístupová kontrola přes vybrané předměty a objekty
- značení možnosti vývozu
- všechny objevené nedostatky musí být odstraněny nebo zmírněny
- navrhované specifikace a verifikace

B2 – strukturovaná ochrana

- bezpečnostní politika jasně definovaná a formálně dokumentovaná
- vymáhání řízení přístupu a povinné přístupové kontroly rozšířeny na všechny předměty a objekty
- skryté skladovací kanály jsou analyzovány pro výskyt a šířku pásma
- pečlivě strukturováno pro zabezpečené kritické a nezabezpečené kritické prvky
- návrh a implementace umožňující komplexnější testování a přezkoumání
- autentifikační mechanismy jsou zesílené
- spolehlivý facility management je poskytován s oddělením administrace a obsluhy
- využívá se přísně rozdělené řízení kontrol

B3 – bezpečnostní domény

- vyhovuje doporučením sledování požadavků
- strukturované k vyloučení zákonů, které nejsou nezbytné k prosazení bezpečnostní politiky
- významné systémové inženýrství směřující k minimalizaci složitosti
- definována role bezpečnostního správce
- audity událostí důležitých z hlediska bezpečnosti
- automatické detekce, oznámení a odezvy na hrozící narušení bezpečnosti
- důvěryhodné procedury pro obnovení systému
- skryté časovací kanály jsou analyzovány pro výskyt a šířku pásma
- příkladem takového systému je XTS-300, předchůdce XTS-400

A – ověřená ochrana

A1 – ověřený design

- funkčně identické jako B3
- oficiální design a ověřené techniky obsahují oficiálně nejvyšší specifikaci
- oficiální řízení a distribuci procedur
- příkladem takového systému je Honywells's Secure Communications Processor SCOMP, předchůdce XTS-400

Mimo A1

- Systémová architektura ukazuje, že požadavky na vlastní ochranu a úplnost referenčního sledování byly implementovány v důvěryhodném výpočetním základu (Trusted Computing Base – TCB)
- Bezpečnostní testování automaticky generuje testovací případy z formálně nejvyšší úrovně specifikace nebo formální požadavky na nižší úrovni
- O formální specifikaci a verifikaci je možné mluvit tam, kde je verifikováno dle TCB až na úroveň zdrojového kódu za použití proveditelných formálních verifikačních metod
- Důvěryhodné vývojové prostředí je to, kde je TCB vyvíjeno v důvěryhodném prostředí pouze důvěryhodným (prověřeným) personálem. [14]

Další nástroj pro hodnocení bezpečnosti systému byl používán v EU od roku 1995, v současné době je také nahrazován nástroji CC. Jedná se o Evropská hodnotící kritéria.

The Information Technology Security Evaluation Criteria (ITSEC)

Je strukturovaný soubor kritérií pro hodnocení počítačové bezpečnosti v rámci produktů a systémů. ITSEC byla poprvé zveřejněna v květnu 1990 ve Francii, Německu, Nizozemsku a ve Spojeném království na základě dosavadní práce ve svých zemích. ITSEC byl z velké části nahrazen *Common Criteria*, která poskytuje podobně definované úrovně hodnocení a implementuje cíle hodnocení koncepce a dokument Security Target.

Common Criteria for Information Technology Security Evaluation (zkráceně **Common Criteria** nebo **CC**) je mezinárodní standard (ISO/IEC 15408) pro certifikaci počítačové bezpečnosti. Aktuálně je ve verzi 3.1. Common Criteria je framework, ve kterém

uživatelé počítačového systému mohou specifikovat jejich bezpečnostní funkcionalitu a jistící požadavky, prodejci potom mohou implementovat a zároveň/nebo se dožadovat bezpečnostních atributů jejich produktů, a testovací laboratoře mohou vyhodnocovat produkty. Jinak řečeno, Common Criteria dává jistotu, že proces specifikace, implementace a hodnocení produktu počítačové bezpečnosti bude řídit přísným a standardizovaným způsobem.

Hodnocení Common Criteria jsou prováděna na produktech a systémech počítačové bezpečnosti.

- Cíl hodnocení - **Target Of Evaluation (TOE)** - produkt nebo systém, který je předmětem hodnocení.
- Ochranný profil - **Protection Profile (PP)** - dokument, typicky vytvořený uživatelem nebo uživatelskou komunitou, který identifikuje bezpečnostní požadavky pro třídu bezpečnostních zařízení (například čipové karty nebo síťové firewally) příslušný danému uživateli ke konkrétnímu účelu.
- Bezpečnostní cíl - **Security Target (ST)** - je dokument, který identifikuje bezpečnostní vlastnosti cíle hodnocení. Může se vztahovat na jeden nebo více PP.
- Bezpečnostní funkční požadavky - **Security Functional Requirements (SFRs)** - specifikuje individuálně bezpečnostní funkce, které mohou produkty poskytovat. Common Criteria poskytuje katalog těchto funkcí. Například může SFR uvádět, jak by uživatel zastupující konkrétní roli měl být autentifikován.
- Bezpečnostní jistící požadavky - **Security Assurance Requirements (SARs)** - popisuje měření získané během vyvíjení a hodnocení produktu k zajištění souladu s prohlášením bezpečnostní funkcionality. Například hodnocení může požadovat, aby všechny zdrojové kódy byly zdrženy v organizačním systému.

Evaluation Assurance Level (EAL) - číselné hodnocení popisující hloubku hodnocení. Každý EAL odpovídá balíčku SAR, který pokrývá kompletní vývoj produktu s danou úrovní striktnosti. Common Criteria sestavilo sedm úrovní, počínaje nejzákladnější EAL 1 (a tudíž nejlevnější na implementaci a hodnocení), končí nejpřísnější EAL 7 (a zároveň nejdražší). [2]

2.2.3 Legislativa

Právní normy, které upravují oblast bezpečnosti IS a její řízení, mimo jiné jsou:

- zákon č. 148/1998 Sb., o ochraně utajovaných skutečností (v roce 2002 novelizován a částečně nahrazen jinými zákony);
- zákon č. 227/2000 Sb., o elektronickém podpisu;
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy;
- zákon č. 101/2000 Sb., o ochraně osobních údajů;
- zákon č. 480/2004 Sb., o některých službách informační společnosti.

Detailní popis těchto norem není předmětem této práce, lze jej však nalézt například na webových stránkách Ministerstva vnitra ČR. [15]

2.3 Metodika bezpečného IS ve společnosti – Systém managementu informační bezpečnosti PDCA

Cyklus PDCA byl původně vytvořen Walterem Shewhart v roce 1930. Následně PDCA pro zlepšování jakosti využil a rozpracoval Edwards Deming.

Metoda se skládá ze 4 po sobě následujících kroků:

P - Plan (plánuj) - cyklus začíná získáváním informací a popisem řešeného problému, které slouží pro připravení plánu. Plán by měl obsahovat jednotlivé činnosti, které je třeba udělat k odstranění problému.

D - Do (dělej) - po vypracování plánu je dalším krokem zavedení popsaných činností.

C - Check (kontroluj) - následuje sledování dosažených výsledků a jejich porovnání s plánem. Jedná se tedy o kontrolu, zda je původní problém skutečně řešen.

A - Act (jednej) - dojde-li k situaci, že se výsledek liší od očekávání a problém není vyřešen, hledejte příčinu problému. Nový plán zaměřte na odstranění příčiny. Je-li problém úspěšně odstraněn, je třeba udělat poslední a závěrečný krok, všechny potřebné změny zavést/standardizovat do procesů nebo systému. Také se samozřejmě přesvědčit, zda změny jsou řádně uplatňovány a součástí běžných každodenních činností.

PDCA byl připraven především pro efektivní řešení a zlepšování výrobních aktivit, procesů a systému. Může být také použit jako jednoduchá metoda pro zavedení změn. Kvalita je obor, kde cyklus zaznamenal hlavní rozvoj a použití v praxi. PDCA by měl být součástí znalostí každého poradce, jež pracuje v oblastech systémů kvality, ekologických systémů nebo zajištění bezpečnosti. [12]

Zásady budování a využívání systému řízení bezpečnosti informací (ISMS – Information Security Management System) stanovené výše uvedenými, v české republice platnými normami (tj. ISO/IEC 27001:2005 atd.) se dají interpretovat různými způsoby v závislosti na velikosti organizace. Jejich podstata však zůstává stejná – informační bezpečnost musí být řízena. Velikost organizace a rozsáhlost jejího systému jsou jedním ze základních parametrů při určování způsobu zavádění ISMS.

Plan, **D**o, **C**heck, **A**ct, tedy Plánování, Implementace, Kontrola (sledování) a Vylepšení jsou 4 kroky, které postupně a cyklicky aplikujeme při zavádění a provozu ISMS dle doporučení normy ISO/IEC 27001 v organizaci jakékoliv velikosti. ISMS je možno aplikovat v malé nebo střední společnosti stejně tak jako v nadnárodním gigantu, který zaměstnává i několik tisíc lidí. Interpretace a implementace jednotlivých doporučení se bude diametrálně lišit podle rozsahu systému, počtu pracovních stanic a zaměstnanců tyto obsluhujících, způsobu a hloubce zpracovaní dat a jejich hodnoty apod. Podívejme se tedy detailněji, jak vypadají jednotlivé fáze nejpoužívanějšího modelu řízení bezpečnosti IS – PDCA.

2.3.1 Plan - plánuj

Tato fáze by měla sestávat z následujících kroků.

Strategie bezpečnosti

Správná volba a způsob prosazení strategie řízení bezpečnosti není jednoduchá záležitost a už v tuto chvíli je vhodné se obrátit na odborníky, pokud tito nejsou ve vlastních řadách. Pro malou firmu je však samotnou strategií už jen to, že se organizace rozhodla řídit bezpečnost svých informací. Jestliže ve středních firmách je dostačující, že se ředitel na své poradě s dalšími vedoucími pracovníky shodne na strategii a ta se začne prosazovat, v malých

firmách je toto ještě jednodušší, kdy od první úvahy ředitele je k započetí realizace stejně daleko, jako od jeho dveří k zasedací místnosti.

Bezpečnostní politika

Proces vytvoření a schválení bezpečnostní politiky je společný pro všechny typy organizací včetně publikování politiky vůči všem zaměstnancům. Také rozsah a obsah dokumentu je velmi podobný. Bezpečnostní politika definuje zásady a pravidla na úrovni cílů a ty jsou zpravidla shodné pro všechny organizace. Musí také obsahovat odkaz na dokument popisující rozsah ISMS, protože systém řízení bezpečnosti v malé ani střední firmě nemusí být zaveden pro celý informační systém (stejně jako systém řízení kvality podle ISO řady 9000). V dokumentu by mela být popsána mj. organizační struktura bezpečnosti, popis bezpečnostních rolí a jejich odpovědností musí odpovídat velikosti systému a počtu uživatelů. Navíc je nutné respektovat zavedenou organizační strukturu a proto je možné pro stejně velké společnosti použít různé modely organizace bezpečnosti.

V malých firmách nemusí být jmenován bezpečnostní ředitel na plný úvazek. Jeho kompetence zpravidla bere na sebe ředitel firmy, který prosazuje bezpečnostní zásady kombinací direktivního a osobního přístupu. Ředitel má na starosti mj. účinnou implementaci bezpečnostní politiky a vyhodnocování (ne analýzu) rizik a rozhodnutí o způsobu jejich pokrytí. Podobně je tomu i s dalšími bezpečnostními rolemi. Administrátor sítě má odpovědnost za praktické provedení bezpečnostních zásad a metodik, o kterých rozhodl ředitel. Některé činnosti z oblasti bezpečnostní dokumentace mohou být v kompetenci vybraného pracovníka, který může mít na starosti také audit. Kumulace práv a pravomocí souvisejících s bezpečností informací a se správou systému je pro malé organizace rizikem, které je nutné přijmout. Pokud má systém pouze několik desítek uživatelů, je možné jednotlivé kompetence rozdělit mezi několik stávajících pracovníku nejen z IT.

Analýza rizik

Znalost bezpečnostních rizik je základním kamenem pro vytvoření a správně řízení ISMS. Proto provedení analýzy rizik je nutná nikoli však postačující podmínka pro všechny organizace. Rozhodnutí, zda provést detailní či jen základní analýzu, je na vedení firmy, nicméně pouze detailní analýza provedená podle vybrané metodiky muže poskytnou podklady pro efektivní výběr a implementaci bezpečnostních opatření. Analýza musí zabrat celý rozsah

ISMS a její hloubka závisí na dostupných zdrojích a požadovaných výstupech. V malé firmě lze provést detailní analýzu (například metodikou CRAMM) za dva až tři týdny. Je možné spolupracovat s konzultační firmou anebo vše udělat za pomoci vlastních (znalých) pracovníků. Zatížení firmy je minimální a počet respondentů nepřevýší 5 lidí. Pro hodnocení dat se vyberou 2-4 zaměstnanci, kteří nejvíce znají charakter a použití definovaných datových aktiv, a administrátor sítě provede hodnocení hroze a zranitelností včetně identifikace existujících protiopatření.

Plán implementace a Prohlášení o aplikovatelnosti

Krokem logicky navazujícím na analýzu a poslední činností v části plánování podle modelu PDCA je vytvoření Plánu implementace a následně Prohlášení o aplikovatelnosti (opatření). Bezpečnostní protiopatření by mela být vybrána na pokrytí zjištěných rizik a způsob jejich výběru je nezávislý na velikosti organizace. Jejich implementace bude rozdílná, ale například pro všechny organizace lze použít BIS-PD 3005 nebo knihovnu protiopatření CRAMM (vše viz dále). Velký rozdíl však je ve způsobu a zejména v rychlosti jejich prosazení. Při výběru bezpečnostních opatření je vždy nutné zohlednit jejich dopad na uživatele a na procesy organizace. V malé firmě je možné jednoduše a rychle změnit téměř jakýkoli proces, aby byl více bezpečný. Stačí vůle ředitele a o změně je rozhodnuto. Čím je organizace vetší, tím je složitější měnit procesy a zavedené postupy. Proto je nutné při výběru protiopatření ve střední firmě více respektovat současný stav. Prohlášení o aplikovatelnosti (opatření) je jedním z dokumentů nutných k certifikaci. Obsahuje informace o implementovaných opatřeních normy, případně dalších protiopatřeních navržených na pokrytí rizik. Hlavním cílem je dokumentovat rozhodnutí, proč dané protiopatření bylo či nebylo vybráno k zavedení. Pokud firma neplánuje být v budoucnosti certifikována, není nutné vytvářet samostatný dokument. Pro malou firmu je plně dostačující, pokud se vhodných způsobem zaznamená rozhodnutí o výběru tak, aby i za několik měsíců bylo jasné, proč není nutné určitě protiopatření implementovat.

Závěrem je nutno podotknout, že zavedení systému řízení bezpečnosti informací je správným krokem pro každou organizaci, která chce zabezpečit své informace a dostatečně řídit rizika. S ohledem na velikost organizace je však nutné velmi rozdílně a hlavně „s citem“ interpretovat jednotlivá doporučení normy. [6]

	Proces	Malá organizace do 15 zaměstnanců, 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců, 3-5 úrovní vedení
P L A N	Plán / projekt bezpečnosti	Schválení strategie/plánu pro bezpečnost	Schválení celkové koncepce bezpečnosti Schválení projektu bezpečnosti
	Bezpečnostní politika	Musí být napsána a schválena vedením Popisuje základní zásady bezpečnosti na úrovni cílu. Definuje organizaci bezpečnosti, odpovědnosti a strukturu bezpečností dokumentace. Obsahuje odkaz na rozsah ISMS	Musí být napsána a schválena vedením Popisuje základní zásady bezpečnosti na úrovni cílu. Definuje organizaci bezpečnosti, odpovednosti a strukturu bezpečností dokumentace. Obsahuje odkaz na rozsah ISMS
	Organizace bezpečnosti	Oddělení/Odbor bezpečnosti: NE Bezp. ředitel: ředitel firmy Bezp. administrátor: administrátor IS Bezp. auditor: odpovědnost delegována na pracovníka (mimo administrátora IS)	Oddělení/Odbor bezpečnosti: ANO (pod IT) Bezp. ředitel: jmenován člen vedení Bezp. manažer: jmenováni 1-3 Bezp. auditor: pracovník interního auditu, nebo delegováno na pracovníka mimo IS Bezp. administrátori: administrátoři částí systému
	Analýza rizik	Nutné provést: ANO. Čas: max. 1 měsíc. Členové projektového týmu: jeden interní pracovník a/nebo konzultant. Respondenti: max. 5. Výstupy: Zpráva o analýze rizik + Implementační plán	Nutné provést: ANO Cas: 3 - 5 měsíců Členové projektového týmu: 2-3 interní pracovníci a/nebo 2-3 konzultanti Resondenti: 5-20 Výstupy: Zpráva o aktivech a dopadech + Zpráva o analýze rizik + Implementační plán
	Výběr opatření a plán implementace	Protiopatření vyplývají z AR Prosazuje: ředitel firmy	Protiopatření vyplývají z AR Prosazuje: ředitel a vedoucí oddělení společně
	Prohlášení o aplikovatelnosti	Dokumentované rozhodnutí, samostatný dokument pouze v případ certifikace	Dokumentované rozhodnutí, samostatný dokument pouze v případ certifikace

Obrázek 4: Shrnutí procesů metody PLAN

2.3.2 Do – dělej

Způsob implementace opatření a metody prosazení

Výběr okruhu opatření ISMS je podobný pro malou i středně velkou firmu. Velký rozdíl však je ve způsobu a zejména v rychlosti jejich prosazení. V malé firmě rozhoduje zpravidla ředitel o tom, kdo bude mít přístup k jakým datum. V malých firmách je běžné, že bezpečnostní ředitel (zpravidla ředitel firmy) rozhodne ráno o změně délky hesla z 6 na 9 znaku. Bezpečnostní administrátor (zpravidla správce sítě) protiopatření zavede ještě před obědem a v rámci příjemně strávené siesty si všichni uživatelé rádi změní heslo. Následující den je protiopatření v systému již zcela zavedeno a automaticky používáno a akceptováno. Taková rychlost implementace je typická pouze pro malé firmy.

Bezpečnostní dokumentace

Značné rozdíly mezi malou a středně velkou firmou jsou ve formě a míře detailu dokumentace bezpečnosti. Není příliš známo, že uvedené normy striktně nevyžadují papírovou formu dokumentace ani její pevnou strukturu, ale ponechávají na preferencích jednotlivých firem, jakou formu a obsah zvolí. Přitom právě obava z přílišné formální administrativy nejčastěji odpuzuje malé a středně velké organizace od zavádění doporučení těchto norem. Dokumentace ISMS požadovaná k certifikaci podle ISO 27001 pochopitelně musí obsahovat určité, taxativně uvedené typy dokumentu, dané jednotlivými kroky procesu ISMS, ale jejich rozsah, obsah a forma muže být překvapivě jednoduchá a flexibilní. Pracovníci malých firem se osobně znají a velká část bezpečnosti je založena na jejich vzájemné důvěře. Není nutné vytvářet složitý systém politik, směrnic a postupu. Postačí stručné pravidlo, že bezpečnostní dokumentace je vedena ve sdílené složce elektronické pošty, definovat role a přístupy zodpovědných osob a nezbytné typy bezpečnostních dokumentu realizovat formou elektronických záznamu, obsahující stručný popis realizace daného pravidla, postupu nebo odpovědnosti. Rozsah a aktuálnost bezpečnostní dokumentace bývá často jedním z klíčových kritérií při posuzování kvality ISMS a míry dosažené shody s požadavky norem.

Program zvyšování bezpečnostního povědomí

Mezi další metody prosazení bezpečnosti v organizacích patří program zvyšování bezpečnostního povědomí v organizacích. Tento krok, jakkoliv komplikovaně znějící, je ve skutečnosti poměrně jednoduchá, levná a účinná metoda, která bývá bohužel mnohdy v malých a středně velkých organizacích opomíjena. Má za cíl zvýšit u všech zaměstnanců informovanost jednak o obecných principech a souvislostech informační bezpečnosti a o konkrétních rizicích, opatřeních, odpovědnostech a pravidlech, vyplývajících ze zaváděného nebo již provozovaného ISMS. Tzv. síla jednoduchosti tohoto opatření spočívá v tom, že program je zaměřen na zaměstnance, kteří jsou často zdrojem bezpečnostních incidentů a kteří mohou, pokud jsou správně informování, svým včasným jednáním šíření a škodám incidentů zabránit. U malých firem postačí, pokud zvyšování bezpečnostního povědomí opřeme o stručné vstupní školení všech zaměstnanců a občasné prodiskutování aktuálních bezpečnostních otázek dle potřeb organizace a vývoje nových potencionálních hrozeb.

Způsob zvládání rizik za provozu

Jedním z hlavních důvodů proč zavádět ISMS, je potřeba zajistit kontinuální proces zvládání a řízení informačních rizik. Základem pro jejich úspěšné řízení je identifikace a analýza všech potencionálních rizik a následné rozhodnutí o způsobu jejich zvládání a sledování v čase. Účelem řízení rizik není veškerá identifikovaná rizika bezezbytku pokrýt (mnohdy s vynaložením neadekvátních zdrojů), ale pokrýt zvolenými opatřeními pouze taková, u kterých je to efektivní. Ostatní rizika muže organizace akceptovat a sledovat, některá muže přenést na jinou organizaci, případně je pojistit. Pouze pokud organizace zná a sleduje všechna rizika související se zabezpečením informací a adekvátně rozhoduje o způsobu jejich zvládání, potom muže prohlásit, že tyto rizika řídí.

Nároky na provoz opatření a zajištění bezpečnosti

Součástí plánu zvládání rizik je i sledování nároku na provoz jednotlivých opatření a celkového zajištění bezpečnosti. Zatímco u malých firem není potřeba plánovat ani vyhrazovat samostatný rozpočet, neboť případný nákup a provoz nezbytných opatření je operativně schválen ředitelem a hrazen dle aktuálních potřeb organizace, u středních a velkých firem je nezbytné provádět alespoň rámcové plánování potřebných finančních

i lidských zdrojů. Z hlediska preferencí při výběru opatření hrají celkové nároky na jejich zavedení a provoz hlavní roli. Zatímco pro malé organizace není překážkou pružně zavádět administrativní a personální opatření i za cenu vyšších požadavku lidské zdrojů, úskalím však bývají finanční náklady na pořízení složitých technologických opatření. U velkých společností lze tyto preference vysledovat obráceně, neboť pro ně bývá snazší pružně zavést nové technologické opatření, než jej nahradit administrativními či organizačními změnami. V případě preferencí středně velkých firem je stav logicky někde uprostřed. Záleží na pružnosti řízení, technologické úrovni a znalostech pracovníku firmy, k jakým typům opatření se budou přiklánět více.

Zavedení opatření DRP a IRH

Poslední důležitou oblastí opatření při zavádění a provozu ISMS je tvorba a údržba Havarijních plánu (DRP – Disaster Recovery Planning) a Postupu řešení bezpečnostních incidentu (IRH – Incident Response Handling). Stejně jako v případě ostatních formálních postupu i zde platí, že pro malé organizace je neefektivní vypracovávat a udržovat podrobné formální havarijní plány. Pro obnovu systému jim plně postačí vytvoření stručného univerzálního havarijního checklistu pro všechny možné případy havárie, který bude obsahovat postup bezpečného vypnutí a restartu technického vybavení a serveru, jednoduchý záznam výsledné konfigurace technologií a aplikací, postup obnovení dat ze záložních médií a seznam kontaktu na interní a externí osoby, které mohou pomoci při výskytu havárie nebo závažného bezpečnostního incidentu. Tyto havarijní postupy by mely být alespoň jednorázově otestovány a poté postačí testy opakovat až při zásadní změně používaných technologií a služeb.

Důležité je v závěru upozornit na fakt, že při implementaci a provozu opatření, zvolených v předchozí fázi Plánuj (Plan) se nezavádí a neprovozují pouze primárně účinná technická a organizační opatření typu: „nastav autentizací mechanizmus“ nebo „eviduj pohyb osob v serverovně“ ale spolu s nimi je třeba myslet na stejně důležitá sekundární řídící opatření, která mají za cíl potřebnou úroveň bezpečnosti dlouhodobě udržovat a komplexně rozvíjet.

	Proces	Malá organizace do 15 zaměstnanců, 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců, 3-5 úrovní vedení
D O	Způsob implementace opatření	Okamžite, rychle, efektivne, bez zbytečné administrativy	Podle významu protiopatření formou projektu nebo direktivním nařízením
	Metody prosazení	Direktivní – Osobní - Neformální Stručné pokyny (email, Intranet) a verbální působení na všechny zaměstnance	Direktivní – Neosobní - Formální Kombinace verbálních pokynu vedoucích a písemných organizačních. Závazné a formální seznámení s nařízeními
	Bezpečnostní dokumentace	Bezpečnostní politika, některé směrnice, občas konkrétní postupy	Bezpecnostní politika a další dokumentace včetne směrnic, postupu, návodu apod.
	Program zvyšování bezpečnostního povědomí	Jednorázové informace dle potřeby. Bezpečnostní minimum součástí úvodního zaškolení.	Nepravidelné pokyny a narízení. Bezpečnostní minimum součástí úvodního zaškolení. Specializovaná školení pro vybrané zaměstnance.
	Způsob zvládání rizik za provozu	Neformální proces, bez speciálních postupu a pravomocí. Pokrytí a kontrola bezprostředně po	Formální proces s rámcově stanoveným postupem a odpovědnostmi. Revize
	Nároky na provoz opatření a zajištění bezpečnosti	Krátkodobé plánování. Není separátní rozpočet. Externí spolupráce není obvyklá.	Krátkodobé a střednědobé plánování Rozpočet v rámci IT/IS Prosazuje se outsourcing
	Zavedení opatření DRP a IRH (Havarijní plány)	Zpravidla řada neformálních havarijních postupu pro jednotlivá aktiva.	Formální univerzální havarijní plán Postupy zvládání bezpečnostních incidentu

Obrázek 5: Shrnutí procesů metody DO

2.3.3 Check – kontroluj

Monitoring provozu

Monitoring provozu klíčových prvku IS a ochranných opatření je základním zdrojem informací pro kontrolu jejich funkčnosti a spolehlivosti. Pokud organizace zavádějící ISMS plánuje v budoucnu i jeho certifikaci, musí vytvářet a shromaždovat záznamy o fungování alespoň těch opatření, která jsou uvedena v Prohlášení o aplikovatelnosti (ty budou předmětem auditu). Bohužel ne všechny typy opatření samy automaticky generují záznamy o činnosti a tak je nezbytné přistoupit i v prostředí malých a středních firem k nepopulárnímu ručnímu generování záznamu u takových opatření, která tuto vlastnost nemají (především organizační a administrativní). Nemusí se přitom zdaleka jednat o únavnou administrativu, protože rozsah a složitost opatření, zvláště u malých a středních firem, nebývá nijak velký. Příkladem toho, co postačí pro audit funkčnosti opatření „bezpečnostní školení uživatelů IS“, jsou seznamy účastníků školení a datum a předmět školení. Povinnost vůči případnému auditu ISMS a certifikaci je splněna. Pro monitoring ICT postačí u malých organizací výchozí nastavení logování dle standardní instalace většiny produktu a jejich ruční namátková kontrola určeným pracovníkem.

Testování funkčnosti opatření

Aby se předešlo problémům při provozu IS, je třeba doplnit i o aktivní a preventivní způsoby, jakými jsou např. aplikační kontroly chyb výpočtu a zpracování dat nebo testování zranitelností, případně penetrační testování systému. Zatímco komplikovanější a časově i finančně náročnější penetrační testování má za cíl simulaci reálných útoků ze zvoleného prostředí a identifikaci možných negativních dopadů na IS, bezesporu jednodušším, rychlejším a levnějším způsobem testování odolnosti vůči útokům je vyhledání a testování zranitelností provozovaných ICT produktu. Oba způsoby mohou být prováděny z interní sítě, nebo častěji z externího prostředí – zpravidla Internetu nebo bezdrátových sítí, což by měly být v případě malých a středních firem hlavní oblasti prevence proti útokům na IS. Protože se v případě penetračního testování jedná o vysoce specializovanou činnost, vyžadující detailní znalosti o technikách a nástrojích hackingu, stejně jako o bezpečnostních slabinách jednotlivých ICT produktu a komunikačních protokolů, bývá tento úkol svěřován specializovaným externím firmám, které mají dostatečné profesní zázemí pro jejich kvalifikovanou realizaci. Naproti tomu testování zranitelností je proces, který si mnohdy

mohou počítačově gramotní uživatelé udělat sami, pomocí dostupných programu nebo využít specializovaných webových služeb.

Audit a kontrola bezpečnostních opatření

Spolu s monitorováním provozu, testováním zranitelností a technicky zaměřeným auditem konfigurace ICT, je další metodou kontroly implementace a provozu IS/ISMS realizace Auditu a kontrol bezpečnosti IS. Obecně lze říci, že audit opatření musí být prováděn v každém typu a velikosti organizace, která provozuje systém řízení nad opatřeními, jinak by neexistovala zpětná vazba o stavu reality vůči plánu a návrhu požadovaného cílového stavu. Každý typ auditu by se mel řídit pravidly ISO 19011:2002 a mel by probíhat dle schváleného ročního i operativního plánu. V případě ISMS by mel audit zahrnovat kontrolu funkčních bezpečnostních i řídících opatření ISMS, která jsou deklarována v Prohlášení o aplikovatelnosti a popsána v bezpečnostní dokumentaci. Audit by mel ověřit, jak jsou realizována v praxi. U malých organizací není třeba vytvářet samostatná oddělení nebo pracovní funkce interního auditora, ale je nutné i v malé organizaci funkci interního auditora dedikovat, alespoň jako přidruženou pracovní náplň nějakému zaměstnanci. Jednou ročně je nezbytné projednání zjištěných výsledku plánovaných auditu i namátkových kontrol s majitelem/ředitelem organizace a následně se všemi zaměstnanci.

Revize adekvátnosti a efektivnosti ISMS

Kromě ověření funkčnosti, spolehlivosti a úplnosti funkčních i řídících opatření je třeba přibližně jednou ročně zrevidovat rozsah, adekvátnost a efektivnost celého ISMS ve vztahu k potřebám, cílům a prostředí organizace. Výsledek této celkové revize ISMS by mel být stejně jako souhrnné výsledky auditu opatření projednán s vedením organizace a pořízeny záznamy o přijatých závěrech. Jelikož se jedná o činnost vyžadující široký přehled a značné zkušenosti z oblasti bezpečnosti informací a implementace ISMS v organizacích, musejí se malé i střední organizace spolehnout na pomoc externích specialistu, stejně jako v případě analýzy informačních rizik v etapě Plan – plánuj.

	Proces	Malá organizace do 15 zaměstnanců, 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců, 3-5 úrovní vedení
C H E C K	Monitoring IS a testování funkčnosti opatření	Namátkový monitoring provozu IS a vyhodnocování logů a záznamů událostí (v papírové i el.podobě). Otestování zranitelností u systémů připojených k Internetu.	Pravidelný monitoring a vyhodnocování logů a záznamů událostí (v papírové i el.podobě). Otestování zranitelnosti u systémů připojených k externím subjektům (třetím stranám).
	Audit a kontrola bezpečnostních opatření	Audit opatření včetně ISMS dle dokumentace a plánu auditu (v případě certifikace ISMS). Iniciuje ředitel, provádí vybraný pracovník jako rozšíření standardní pracovní náplně. Namátková interní kontrola stavu opatření.	Audit opatření včetně ISMS dle dokumentace a plánu auditu (v případě certifikace ISMS). Bezpečnostní technický audit nastavení klíčových ICT systémů. Namátková interní kontrola stavu opatření.
	Revize adekvátnosti a efektivnosti ISMS	Rámcová revize procesu ISMS a vyhodnocení aktuálnosti, efektivnosti a adekvátnosti opatření. 1 denní workshop s využitím externího konzultanta.	Roční podrobná revize procesu ISMS a stavu opatření s využitím externího konzultanta. Porovnávání stávajících opatření s novými trendy a vývojem hrozeb a zranitelností.

Obrázek 6: Shrnutí procesů metody CHECK

2.3.4 Act – jednej

Vyhodnocení fáze Check - kontroluj

Základním předpokladem pro správné rozhodnutí „co a jak dál“ by vždy měly být co nejpřesnější a nejúplnější informace o aktuálním stavu a cílech organizace. Informace o aktuálním stavu týkající se monitoringu provozu, evidence chyb a bezpečnostních incidentu, výsledku testování funkčnosti a spolehlivosti implementovaných opatření, výsledku testování zranitelností a výsledky interních i externích auditů poskytuje předcházející fáze Check-kontroluj. Vyhodnocení těchto informací provádí v malých firmách pracovník pověřený činností bezpečnostního manažera (jako přidruženou činnost ke své pracovní náplni). Výsledky svého šetření by měl minimálně jednou ročně předložit majiteli, případně řediteli organizace a společně provést jejich analýzu a vyhodnocení.

Identifikace a analýza neshod

I když byla revize výsledku auditu zahrnuta již do předcházejícího kroku, je vhodné tuto činnost popsat podrobněji. Identifikace a analýza neshod má za úkol rozebrat výsledky interního i případného externího auditu a posoudit, které z nalezených neshod jsou skutečné, které pouze potenciální a vyřadit nesprávně identifikované neshody. Toto rozhodnutí je opět vhodné zaevidovat formou tabulky. Nakonec je pro odstranění skutečně identifikovaných neshod třeba navrhnout nápravná opatření a pro zabránění opakovaného výskytu skutečných i potencionálních neshod v budoucnu je třeba navrhnout preventivní opatření. Jejich výběr, implementace a ověření funkčnosti je již náplní dalších paralelních PDCA procesu (koleček), které jsou spuštěny pro každé nově navržené opatření. U malých organizací provede tuto analýzu neshod majitel, případně ředitel organizace, ve spolupráci s pracovníkem pověřeným funkcí bezpečnostního manažera. S výsledným rozhodnutím je vhodné seznámit všechny zaměstnance. Implementace těchto rozhodnutí bývá velmi rychlá a flexibilní. Pokud malá firma usiluje o certifikaci ISMS, je vhodné obrátit se pro pomoc na externího konzultanta, případně zrealizovat srovnávací audit procesu ISMS vzhledem k ISO 27001 externí specializovanou firmou a s její pomocí navrhnout potřebná nápravná opatření pro dosažení souladu.

Nesprávná a preventivní opatření

Nápravná opatření slouží k odstranění skutečně nalezených nedostatku a chyb, spojených s implementací a provozem ISMS a k zabránění jejich dalšímu trvání (opakování). Jedná se například o neúplnou implementaci opatření zvolených v Prohlášení o aplikovatelnosti opatření, o chybějící dokumentaci těchto opatření, o nedostatečné proškolení pracovníků zainteresovaných v procesu ISMS apod. Preventivní opatření jsou vybírána s cílem zabránit výskytu potencionálních neshod v budoucnu, tedy za účelem eliminace příčin, které by mohly vést ke vzniku reálné nežádoucí situace a reálné neshody. Příkladem takové potencionální neshody muže být například nedodržení oddělení rolí u některých činností a opatření ISMS nebo nedůsledné provádění potřebných monitorovacích a kontrolních činností. Pro malé organizace je typická rychlá praktická změna bez byrokratických průtahů a příklon především k organizačním a personálním opatřením, jejichž „pořízení a zavedení“ bývá pro majitele malých firem nejpřijatelnější.

	Proces	Malá organizace do 15 zaměstnanců, 1-2 úrovně vedení	Střední organizace do 150 zaměstnanců, 3-5 úrovní vedení
A C T	Vyhodnocení fáze Check - kontroluj	Revize zejména bezpečnostních incidentů, chyb a průběhu jejich řešení (dle potřeby). Revize penetračního a zkušebního testování, pokud bylo realizováno. Revize výsledků ročního auditu.	Pravidelná revize incidentů, chyb a průběhu jejich řešení. Revize penetračních a dalších typů testů. Revize výsledků auditu. Revize nápadů a podnětů ke zlepšení. Revize adekvátnosti a efektivnosti ISMS.
	Identifikace a analýza neshod	Identifikace a evidence možností zlepšování, reálných neshod a potenciálních problémů. Interpretace a okamžitý návrh opatření ředitelem / majitelem.	Identifikace a evidence možností zlepšování, reálných neshod a potenciálních problémů. Interpretace výsledků kontrol interním auditem s využitím externích odborníků. Jednoduchý projekt pro návrh opatření.
	Nesprávná a preventivní opatření	Přednostní výběr jednoduchých organizačních a personálních opatření, bez nutnosti investic. Rychlé zavedení dostupných opatření do praxe.	Výběr organizačních opatření podpořených technologiemi a nástroji. Testování opatření před uvedením do praxe. Aktualizace bezpečnostní dokumentace.

Obrázek 7: Shrnutí procesů metody ACT

2.4 Principy provádění bezpečnostního auditu

Ještě než bude proveden samotný audit, je potřeba zmínit principy a následný postup, který bývá typický při samotném jeho vykonávání.

Principy auditu:

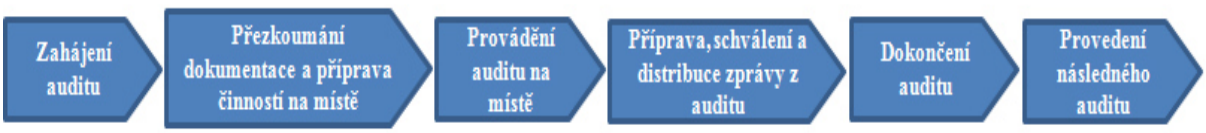
Provádění auditů a vlastní činnost auditorů jsou spojeny s respektováním a dodržováním řady zásad a pravidel. Právě tyto zásady činí z auditu efektivní a hlavně spolehlivý nástroj pro podporu účinného řízení, který poskytuje nenahraditelné informace, nutné pro trvalé zlepšování systémů řízení. Dodržování následujících zásad je předpokladem pro zajištění odpovídajících, dostatečných a opakovatelných závěrů:

- **Etické chování** – důvěryhodnost, jednotnost, důvěrnost a diskrétnost vztahu auditora a auditované činnosti při manipulaci s informacemi a daty.
- **Spravedlivá prezentace** – zjištění, závěry a zprávy z auditu musí být vždy pravdivé a musí přesně popisovat veškeré činnosti, provedené v jeho průběhu.
- **Povinnost profesionálního přístupu** – auditor musí mít vysokou odbornou a profesní způsobilost a musí využívat své odborné zkušenosti, dané nejlepší vžitou praxí v oblasti ICT.
- **Nezávislost** – auditor musí být naprosto nezávislý na auditované činnosti a prováděný audit je důsledně veden s cílem nalézt objektivní stanovisko.
- **Průkaznost** – veškeré závěry a informace z provedeného auditu musí být zpětně ověřitelné.

Popis auditu:

Nyní bude popsán samotný průběh auditu IS/ICT trochu podrobněji. Schéma je znázorněno na obrázku č. 8.

Typicky je možno audit rozdělit do následujících částí (doporučení dle ISO 191):



Obrázek 8: Typický průběh auditu bezpečnosti

- **Zahájení auditu** – se věnuje zejména jmenováním vedoucího auditorského týmu, definici cílů, rozsahu, předmětu a kritériím auditu, hodnocení proveditelnosti auditu, vytvoření auditního týmu a navázání prvního kontaktu s auditovanou osobou.
- **Přezkoumání dokumentace a příprava činností na místě** – všechny audity by se měly opírat o základní znalost prostředí. Tato fáze auditu slouží k prostudování existující dokumentace (včetně elektronických dokumentů), která je základem pro návrh účinného plánu auditu včetně hrubého rozvržení úkolů pro jednotlivé členy pracovního týmu. Dokumenty jsou posuzovány vzhledem k cílům auditu a navrženým kritériím auditu. Součástí této fáze auditu je též příprava různých pracovních dokumentů, auditního týmu (např. dotazníky, podklady pro řízené rozhory, plány tvorby datových vzorků, způsob jejich vyhodnocování apod.).
- **Provádění auditu na místě** – je jádrem celého auditu, kdy dochází k vlastnímu sběru informací o skutečném fungování systému, k ověřování zjištěných skutečností a ke shromáždění důkazů. Hlavní činnosti v této části jsou zejména:
    - Úvodní setkání s auditovanou stranou (představení členů týmu, cílů a rozsahu auditu, stanovení způsobů komunikace, zajištění místa a potřebných zařízen apod.)
    - Komunikace s auditovanou stranou (způsob referování o postupu auditu, řešení problémů a případných změn)
    - Určení rolí a odpovědností průvodců a pozorovatelů (nejsou součástí týmu, obyčejně jde o osoby určené auditovanou stranou pro asistenci auditorům)
    - Shromažďování a ověřování dokumentace
    - Formulace nálezů (nálezy mohou potvrdit soulad nebo nesoulad s určenými kritérii; v případě, že je cílem auditu i návrh opatření na zlepšení, formulují se nálezy včetně těchto opatření)
    - Příprava závěrů auditu (auditorský tým předběžně projednává formulované nálezy auditu a diskutuje další postup auditu)
    - Organizace uzavřeného jednání o závěrech auditu (auditorský tým společně se zástupci auditované strany prezentují výsledky auditu a řeší opatření pro případ, že existují nějaké důvody, vedoucí ke snížení spolehlivosti závěrů auditu)
- **Příprava, schválení a distribuce zprávy z auditu** – pro zpracování zprávy z auditu je důležité důkladné vyhodnocení všech zjištěných skutečností včetně zvážení

možných negativních dopadů a závěrů auditu na organizaci a dalších vzájemných souvislostí. Tato práce je základem pro formulaci stručné a výstižné zprávy z auditu, která je vlastnictvím auditované strany, a proto musí být zachována předem určená pravidla jejího utajení. Výstupní zpráva z auditu by měla poskytovat úplný, pravdivý, stručný a srozumitelný záznam o auditu. Zpráva o auditu by měla obsahovat:

- Identifikaci auditorské strany
- Identifikaci vedoucího auditora a jeho týmu
- Cíle auditu
- Kritéria auditu
- Rozsah auditu, zvláště identifikaci auditovaných organizačních a funkčních jednotek nebo procesů a časový úsek, ve kterém audit proběhl
- Data a místa, ve kterých proběhla šetření v místě zákazníka
- Nálezy auditu a doporučení
- Závěry auditu

Kromě výše uvedených údajů by měla zpráva z auditu podle potřeby také zahrnovat:

- Plán auditu
- Seznam lidí, kteří spolupracovali na straně zákazníka s auditory
- Přehled realizovaných akcí/procesů auditu a případné okolnosti, které vedly ke snížení spolehlivosti závěrů auditu
- Potvrzení o tom, že bylo dosaženo definovaných cílů auditu
- Přehled oblastí, které byly zahrnuty v původním plánu a nebyly při auditu provedeny
- Popis nevyřešených rozdílných názorů mezi auditorským týmem a auditovanou stranou
- Přehled doporučení ke zlepšení, pokud byly součástí cílů auditu
- Odsouhlasený plán realizace nápravných doporučení (pokud je výsledkem auditu)
- Prohlášení o zachování mlčenlivosti o získaných údajích
- Seznam příjemců auditorské zprávy a způsob jejího doručení

- **Dokončení auditu** – je důležité pro vlastní auditorský tým, aby si sám vyhodnotil úspěšné stránky auditu i ty méně zdařilé. Důsledná a objektivní sebereflexe je důležitým nástrojem optimalizace i pro auditory.

3 Analýza stávajícího stavu ve firmě

3.1 Charakteristika stávajícího stavu firmy

Při provádění bezpečnostního auditu je poznání prostředí dané organizace nezbytnou součástí. Nejprve je potřeba se zaměřit na oblast, ve které společnost podniká a na její základní rozvrstvení. Poté je třeba získat bližší informace o zařízeních, které ke své činnosti organizace používá a dále se věnovat samotnému provozu těchto zařízení. Při této příležitosti jsem se rozhodl pro sestavení několika základních bodů, pokrývající oblasti základní infrastruktury podniku, klientských stanic, počítačových sítí, serverů, zálohování dat, a tím získat základní přehled stavu ICT.

1) O firmě:

Fashion Arena Center Management sestává ze šesti interních zaměstnanců: Ředitel, Marketing Online-Development Mgr., Retail Mgr., Facility Mgr., Office Mgr., Receptionist / Team Assistant. Ostatní pozice, které jsou mimo FAOC (Fashion Arena Outlet Centrum), jsou outsourcovány.

2) Klientské stanice:

- **Operační systémy klientských stanic**

Převážně Windows 7 Professional, cca 1-2 PC mají Windows Vista Business.

- **Používaný software pro práci**

MS Office, Internet Explorer / Google Chrome, Adobe Reader, Adobe Photoshop.

- **Zabezpečení stanic**

Antivirus a firewall ESET Endpoint Security / ESET Smart Security s centrálním řízením ESET ERA. Antispam v rámci poštovního serveru MS Exchange.

- **HW, které mají zaměstnanci k dispozici**

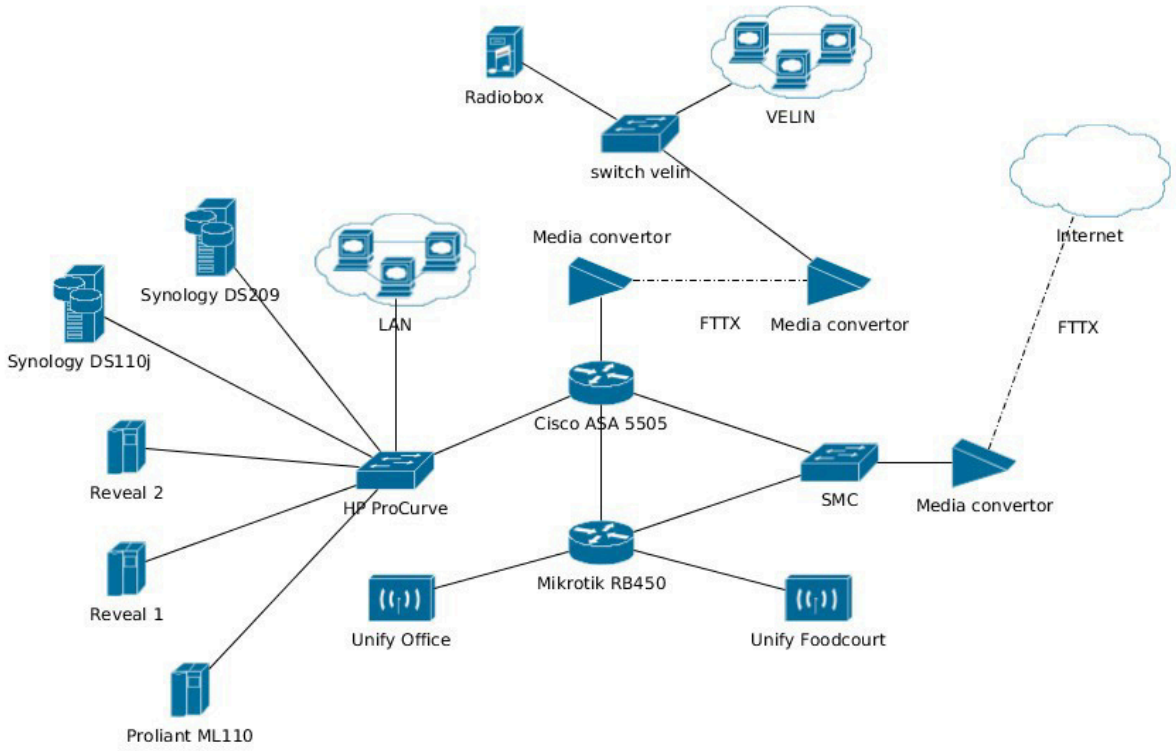
PC stanice značky HP (převážně Core 2 Duo), notebook značky Lenovo (starší Pentium), notebook značky Dell, tiskárna LaserJet 2840, tiskárna OKI C830, tiskárna Brother.

- **Nastavení práv**

Počítačové a uživatelské účty jsou centrálně řízeny z doménového řadiče skrze Active Directory. Nastavení stanic řízeno přes Group Policy. Uživatelé standardně nemají administrátorská práva.

3) Sítě

- **Schéma sítě**



Obrázek 9: Schéma sítě FAOC

- **Stručný popis sítě**

Celkem 7 stanic (5 workstations, 2 notebooky) je připojeno k neřiditelnému switchi HP ProCurve pomocí strukturované kabeláže. Do téhož switche jsou připojeny celkem 3 servery, 2 routery (Cisco a Mikrotik) a 2 NAS (Synology). Router Cisco slouží coby brána pro přístup na internet, firewall a jako VPN koncentrátor. Router Mikrotik slouží jako brána pro wifi včetně směrování VLAN (z licenčních důvodů pro tento účel nešlo použít Cisco, proto druhý router). V budově existuje ještě oddělená síť pro velín, kde jsou připojeny některé systémy třetích stran (např.: kamerový systém, rozhlas, přehrávání hudby atd.). Tato síť je připojena v módu demilitarizované zóny k routeru Cisco.

- **Výrobci síťových prvků**

Cisco, Mikrotik, HP, Ubiquity.

- **Technologie připojení k internetu – rychlost připojení**

FTTX připojení, 20Mbit symetricky.

- **Technologie připojení zaměstnaneckých notebooků (stanic) k internetu**

LAN (1Gbit Ethernet), wifi (802.11bgn).

- **Wifi připojení – typ šifrování + kdo má přístup k heslu**

Wifi dle standardu 802.11bgn se šifrováním WPA2-Personal pro přístup do vnitřní sítě, popřípadě žádné šifrování pro hotspot přístup na internet. Heslo je k dispozici zaměstnancům u facility managera.

- **Zabezpečení sítě**

LAN síť je chráněna firewallem na routeru Cisco. Wifi síť je řízena pomocí hifi controlleru, který rozděluje wifi klienty do VLAN dle použitého ESSID a zadaného hesla. Směrování VLAN pak provádí router Mikrotik. V budově jsou vysílány celkem 3 wifi sítě. První je šifrovaná síť pro zařízení zaměstnanců s přímým přístupem do vnitřní sítě, druhá je šifrovaná síť pro oficiální návštěvy vedení (pouze internet) a třetí síť je hotspot přístup pro zákazníky centra. Hotspot síť je propojena s uvítacím webem, který mimo jiné slouží k registraci mailu zákazníků, kteří chtějí využít připojení k internetu.

- **Zodpovědná osoba za chod sítě**

Chod sítě je monitorován firmou Netkeepers s.r.o., Pod strojírnami 706/5, Vysočany, 190 00 Praha 9, IČO: 24231983, DIČ: CZ24231983 v rámci servisní smlouvy s FAOC.

4) Servery

- **Počet serverů**

Celkem 3 servery.

- **Kde se servery nachází**

V technologické místnosti v kancelářích managementu centra.

- **Operační systém serverů**

Dva servery jsou spravovány třetí stranou (pravděpodobně Linux). Třetí server je virtualizovaný. Pro virtualizaci byl použit operační systém Ubuntu 12.04 LTS 64bit ve spojení s technologií KVM. V zatím jediném virtuálním stroji běží operační systém MS Windows Server 2011 SBS.

- **Rychlost propojení s vnitřní a vnější sítí**

1GBit do LAN, 20Mbit na internet.

- **Výrobce serverů a jejich parametry**

Dva servery jsou spravovány třetí stranou a jsou tedy z naší strany neznámé. Třetí server je HP Proliant ML110 G7 (Xeon E3-1220, 8GB RAM, HDD 2x250GB v RAID1).

- **Přístupy k serverům**

Fyzický přístup mají teoreticky všichni zaměstnanci. Elektronický přístup k administraci serveru mají technici firmy v rámci servisní smlouvy s FAOC. Administrátorský přístup má rovněž facility manager FAOC.

5) Zálohování

- **Kam se data ze serverů přenášejí**

Data se přenášejí na NAS.

- **Jak často se data zálohují**

Denně.

- **Typy prováděných záloh**

O víkendu se provádí úplná záloha, přes týden diferenciální.

- **Kam jsou ukládány zálohy samotné**

Opět na NAS.

3.2 Analýza rizik

V této kapitole bude proveden bezpečnostní audit společnosti. K tomu bude nejprve zapotřebí zjistit, co je předmětem samotné ochrany, tzn., že bude třeba nalézt všechna aktiva, kterými firma FAOC disponuje. Dále bude třeba určit, před čím aktiva chceme ochránit. Bude tedy stanoven seznam hrozeb, které budou v další části rozebrány. Poté bude třeba určit význam jednotlivých aktiv. Podobně je třeba určit dopad vybraných hrozeb. Na základě těchto informací lze vypočíst rizika pro jednotlivá aktiva a z nich poté vyvodit adekvátní návrhy na jejich snížení.

3.2.1 Identifikace aktiv

Nejprve bylo potřeba stanovit oblasti jednotlivých aktiv. Tyto oblasti byly rozděleny do následujících kategorií: data (informace), hardware, software, komunikační zařízení, dokumenty a personál.

Data (informace) – Do skupiny informací byla zařazena účetní data, která obsahují zejména faktury a pokladní doklady, evidence zaměstnanců, jako jsou například jejich pracovní výkazy, docházka, záznamy o dovolené, výplatní záznamy a jiné.

Hardware a software – Hardware se dá rozdělit do dvou skupin, a to podle toho kde je umístěn, případně kdo jej používá. Mimo toto rozdělení stojí sbírka fyzického vybavení, která byla vytvořena během působení firmy. Jedná se o kolekci různých médií, které obsahují potřebné ovladače, testovací hardwarové komponenty a jiné servisní pomůcky. Do kategorie software je možno zařadit veškerý software, se kterým firma disponuje.

Komunikační zařízení – Komunikační zařízení jsou taktéž důležitou skupinou aktiv. Jejich rozdělení je opět dle umístění a výjimku tvoří telefonní síť, která je tvořena mobilními telefony.

Dokumenty – V oblasti dokumentů byla identifikována aktiva v oblasti účetnictví. Firma outsourcuje účetní, u které jsou uloženy všechny fyzické dokumenty. Dalším aktivem

jsou smlouvy se zaměstnanci, vzory smluv, které se uzavírají při poskytování služeb, pronájmu obchodních jednotek a jiné dokumenty. Dále identifikovaná aktiva jsou záruční listy a zápisy porad.

Personál – Zde je možno zařadit tzv. know-how firmy a znalosti jednotlivých zaměstnanců. Zatímco know-how jsou určité technologické a informační předpoklady, osobní znalosti nejsou nikde zaznamenány a se ztrátou zaměstnance o ně firma přichází.

3.2.2 Ohodnocení aktiv

Z hlediska potřeby určení důležitosti aktiv byl použit následující postup. Byla zavedena klasifikace vyjadřující dopad ztráty dané vlastnosti aktiva, která je shrnuta v následující tabulce.

Hodnocení	Význam
1	Žádný dopad na organizaci
2	Zanedbatelný dopad na organizaci
3	Potíže či finanční ztráty
4	Vážné potíže či podstatné finanční ztráty
5	Případné existenční potíže organizace
N	Respondent nedokázal odpovědět

Hodnotily se následující vlastnosti aktiv:

- **Dostupnost** – zajištění, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby.
- **Důvěrnost** – zajištění, že informace jsou přístupné nebo sděleny pouze těm, kteří jsou k tomu oprávněni.
- **Integrita** – zajištění správnosti a úplnosti informací.

K celkovému ohodnocení aktiva byl použit výpočet dle vzorce:

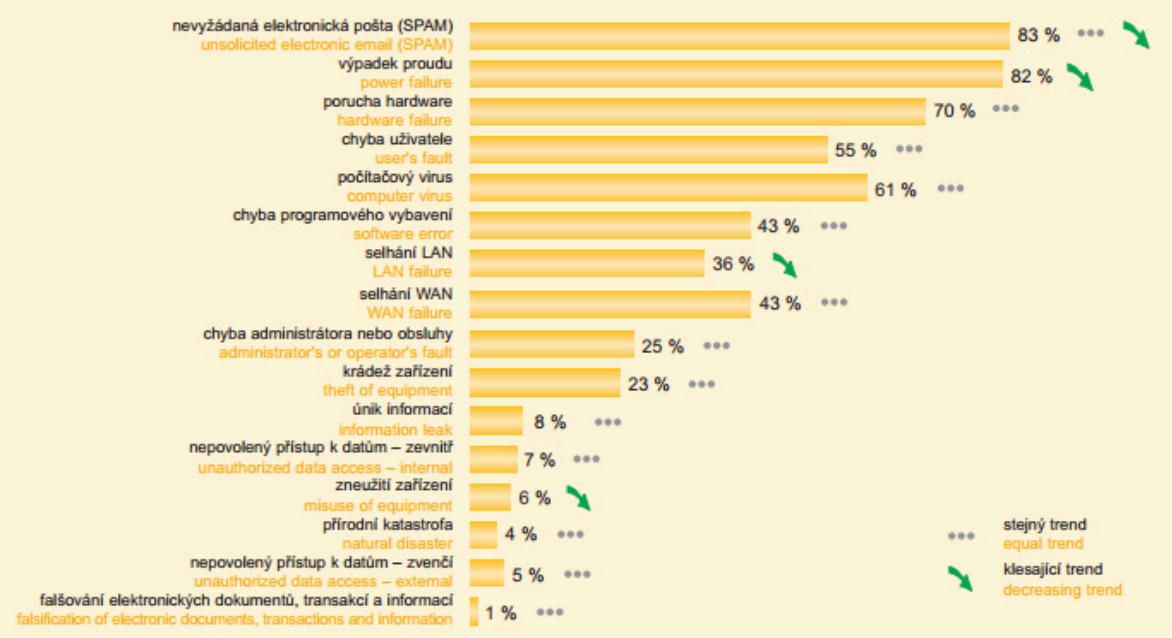
$$\frac{\text{Dostupnost} + \text{Důvernost} + \text{Integrita}}{3}$$

Výjimku při hodnocení tvoří image organizace, u kterého číslo udává, jaký význam pro organizaci má obecně. Cílem bylo získat dobrý pohled na vnímání bezpečnosti na různých pracovních pozicích. Pro hodnocení byl konkrétně osloven zástupce firmy Netkeepers s.r.o.,

jakožto IT podpora společnosti FAOC, ředitel a facility manager této společnosti. Samotná evaluace aktiv bude provedena v kapitole č. 4.

3.2.3 Identifikace hrozeb

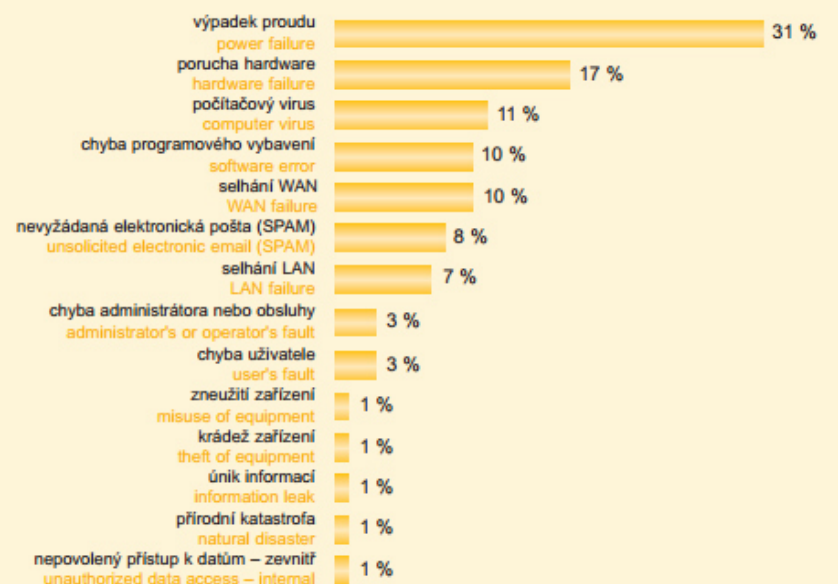
Aby bylo možno stávající zranitelnosti a hrozby vyhodnotit a zaměřit se na ty s nejvyšší pravděpodobnostní, budu vycházet ze zprávy PSIB ČR2009 (Průzkum stavu informační bezpečnosti v ČR roku 2009), kterou provedla společnost Ernst & Young ve spolupráci s časopisem DSM a Národním bezpečnostním úřadem. [13]



Obrázek 10: Výskyt bezpečnostních incidentů za poslední dva roky a vnímání trendu jejich výskytu

3.2.4 Frekvence výskytu bezpečnostních incidentů a jejich dopady

Virus vrací úder. To je asi nejvýstižnější komentář k tomuto grafu. Po posledních dvou ročnících, kdy byly diskutovány změny na „virové“ scéně, úspěchy a standardizaci nasazení antivirových technologií, se viry opět dostávají na scénu jako třetí typ incidentu s nejzávažnějším dopadem. [13]



Obrázek 11: Bezpečnostní incidenty s nejzávažnějším dopadem

Tyto informace byly prezentovány zástupci firmy Netkeepers s.r.o., jakožto IT podpora společnosti FAOC, který toto pořadí bezpečnostních incidentů potvrdil.

3.2.5 Určení zranitelnosti jednotlivých bezpečnostních hrozeb

Výpadek proudu má vliv na všechna aktiva, která jsou dostupná elektronickou cestou. Všechna aktiva z kategorie informace jsou tedy touto hrozbou zranitelná. Pokud se jedná o výpadek v okolí společnosti FAOC, zasažena jsou všechna výše uvedená aktiva s výjimkou evidence chodu firmy, záloh, analýzy cen produktů a certifikátů, které jsou uloženy na jiných místech. Při výpadku proudu v kanceláři obvykle hrozí pouze výpadek spojení do internetu, neboť i někteří zaměstnanci používají k práci notebooky. Dle lokality výpadku jsou pak zasažena odpovídající aktiva z oblasti hardwaru, softwaru a komunikačních zařízení. Mimo dostupnost však obvykle nemá výpadek proudu dopad na jiné kvality aktiv. Vzhledem k vlivu na nedostupnost služeb však ohrožuje image společnosti.

Porucha hardware může mít dopad jak na hardwarové vybavení, tak na aktiva z oblasti informací a dat. Velký problém by též působil výpadek komunikačních zařízení. V závislosti na konkrétní poruše by mohla být též zasažena aktiva z oblasti softwaru. Může se jednat o zákaznická data, účetní data, konfigurační soubory, zálohy, certifikáty, vybavení v datových centrech, vlastní vyvinuté aplikace, skripty. Při těchto poruchách dochází též ke ztrátě image společnosti.

Dalším z řady vybraných bezpečnostních incidentů mohou být chyby v programovém vybavení. Ty jsou závažné zejména pro aktiva v elektronické podobě. Samotné ukládání dat na úložná média je zajištěno stabilními a prověřenými ovladači a souborovými systémy. Firma na serverech používá zásadně software, který je výrobci označen jako stabilní. Pokud by se v něm však objevily nějaké chyby, byla by zasažena databáze statistik a logů, antispamová databáze a zálohy. Tím by taktéž utrpěla image společnosti.

Nevyžádaná pošta je hrozbou především kvůli zátěži, která je spojena s jejím zpracováním. Ohrožena mohou být tak nejrůznější data o zákaznících či pronajimatelích, která mohou být nedostupná.

V případě výpadku WAN se jedná o stejný problém jako u výpadku proudu. Všechny servery jsou totiž připojeny jedinou WAN linkou. Výpadkem jsou tedy ohrožena stejná aktiva. V případě výpadku LAN jsou ohrožena zejména aktiva, která se rozprostírají přes několik serverů. Zde se jedná o účetní data, seznam zákazníků, pronajimatelů a data s nimi související.

Při nepovoleném přístupu k datům zvenčí dochází k ohrožení všech aktiv z oblasti informací a softwaru a zejména image společnosti. Nejvíce zranitelná jsou především zákaznická data, neboť z principu musí být nejlépe dostupná.

3.2.6 Základ pro určení kritických míst

Z obrázku č. 11 vyplývá, že mezi nejčastější bezpečnostní incidenty se závažným dopadem patří výpadek proudu, porucha hardware, počítačový virus a chyba programového vybavení. Kapitola se bude zaměřovat na čtyři nejčastější uvedené bezpečnostní incidenty s nejzávažnějším dopadem z předchozí podkapitoly. Výsledkem by měl být základ pro určení kritických míst a pro návrh snížení jejich rizik.

Výpadky proudu

FAOC má své servery uloženy v technologické místnosti svých kancelářích managementu centra, ta ovšem disponuje několika záložními zdroji elektrické energie. V záloze jsou i motorgenerátory, které garantují bez tankování provoz po 24 hodin. Výpadek proudu v kanceláři není výjimkou. Kancelář je však vybavena UPS jednotkou. Bezdrátový

přístupový bod však podobným způsobem zajištěn není a při výpadku proudu tedy nefunguje bezdrátová síť, potažmo je nedostupný internet.

Poruchy hardwaru

U nejčastějších poruch hardwaru se můžeme setkat s problémy u pevných disků nebo serverů. Takové poruchy by měly dopad na zákaznická data, účetní data, konfigurační soubory, zálohy, certifikáty, vlastní vyvinuté aplikace či skripty. V současné době jsou všechna tato aktiva s výjimkou záloh uložena na diskových polích RAID úrovně 1. V případě záloh je použitý RAID úrovně 5.

V případě jiné hardwarové poruchy může být ohroženo přímo vybavení. Například zkrat či nedostatečně chlazené komponenty serveru mohou v extrémním případě vyvolat požár. Technologická místnost, kde se všechny servery nacházejí, mají protipožární systémy plynového hašení.

Počítačový virus

Třetím uvedeným incidentem s nejzávažnějším dopadem jsou počítačové viry. Jak ovšem bylo zjištěno, v případě společnosti FAOC nemají s viry větší problémy. Navržená bezpečnostní politika však určuje přesná pravidla chování uživatelů, administrace systémů a implementace a použití antivirového řešení. Z tohoto pohledu lze konstatovat, že spolu s navrženou bezpečnostní politikou je zabezpečení proti virovým nákazám dostatečné. Problematika počítačových virů se však zároveň týká i pořizování pravidelných záloh. Tuto situace ve firmě lze prohlásit za uspokojivou.

Chyby v programovém vybavení

Chyby v programovém vybavení je třeba prozkoumat odděleně pro různá aktiva. Například chyby v souborovém systému by měly dopad na všechna aktiva, která jsou uložena na úložných médiích. Taková pravděpodobnost chyby je však nízká, neboť souborové systémy, které se pro ukládání dat používají, jsou výrobci a uživateli velice důkladně testovány. Větší pravděpodobnost výskytu chyb spatřuji v softwaru, který je často aktualizován. V případě firmy FAOC se jedná zejména o běžné uživatelské softwary pro práci, jako jsou MS Office, Internet Explorer, Google Chrome, Adobe Reader a Adobe Photoshop.

4 Návrh inovace bezpečnosti

4.1 Vyhodnocení aktiv

Tabulka shrnuje výsledky hodnocení. Sloupce označené jako Z, Ř, F vyjadřují, kdo dané aktivum hodnotil. Jedná se o již zmiňovaného zástupce firmy Netkeepers s.r.o., ředitele společnosti a facility managera v tomto pořadí.

Aktivum	Z	Ř	F
Data (informace)			
Účetní data z ekonomického sw	N	3	4
Evidence chodu firmy (docházka, pracovní výkazy)	4	3	2
Analýzy cen produktů (náklady, výnosy)	4	3	3
Seznam zákazníků	4	3	3
Antispamová databáze	2	3	2
Data zákazníků	5	4	5
Konfigurační soubory	5	3	4
Zálohy	5	3	4
Certifikáty	5	4	3
Hardware			
Vybavení kanceláře	3	4	2
Vybavení technologické místnosti	5	5	4
Servisní média (sbírky ovladačů, svobodných programů)	3	2	2
Software			
Používané aplikace	5	5	4
Skripty (automatizované úkony na serverech)	4	4	3
Komunikační zařízení			
Struktura sítě FAOC (modemy, switche)	5	5	4
Vnitřní síť kanceláře	4	3	2
Telefonní síť (telefony zaměstnanců, hotline)	3	4	2
Dokumenty			
Účetní doklady (papírové účetnictví)	N	4	4
Smlouvy, vzory smluv a jiných dokumentů	N	3	4
Záruční listy	N	2	3
Zápisy porad	3	1	2
Personál			
Opakované postupy	3	3	3
Vlastní znalosti	3	5	4
Ostatní			
Image organizace	3	5	3

Obrázek 12: Celkové hodnocení aktiv vybranými zaměstnanci (1 – žádný dopad na organizaci, 2 – zanedbatelný dopad na organizaci, 3 – potíže či finanční ztráty, 4 – vážné potíže či podstatné finanční ztráty, 5 – případné existenční potíže organizace, N – respondent nedokázal odpovědět)

Z průzkumu je vidět, že nejvíce hodnocenými aktivy jsou data zákazníků, hardwarové vybavení technologické místnosti, struktura sítě FAOC pokrývající rozsáhlý komplex společnosti včetně management centra, využívané aplikace potřebné k chodu společnosti. Naopak mezi nejméně cenné průzkum zařadil antispamovou databázi, servisní média a zápisy porad. Poměrně velký rozdíl v hodnocení je možné sledovat u vnitrofiremních dat - evidence chodu firmy a zápisy porad.

4.2 Návrhy a doporučení

V této kapitole budou shrnuta doporučení, která mají za cíl snížit rizika nalezená v předchozí části. U každého opatření budou stanoveny přibližné náklady na provedení.

Výpadky proudu

Následkům, které mohou být způsobeny výpadkem proudu, se může společnost efektivně a levně bránit instalací dostatečně dimenzovaných UPS jednotek u všech klíčových zařízení. Tím lze předejít náhlému vypnutí všech systémů bez předchozí přípravy a tím případné ztrátě dat. Protože se v případě společnosti FAOC nejedná o zdravotnické zařízení či jiné zařízení, jehož provoz ovlivňuje širokou veřejnost, lze zkonstatovat, že případná instalace a následná údržba záložního naftového agregátu pro výrobu elektrické energie v době jejího výpadku by nebyla ekonomicky opodstatněná. Bylo také zjištěno, že v dané oblasti nejsou elektrické výpadky častou a hlavně dlouhodobou záležitostí. Případná výše investice by se pohybovala mezi 50.000 Kč až 100.000 Kč jen za dieselový agregát s možností automatického elektrického spuštění z vlastního akumulátoru. Navíc by se musela připočítat cena za nějaký řídicí systém. Problémem však zůstává, že takový generátor by stejně nedokázal pokrýt elektrickou spotřebu celé firmy, takže by umožnil pouze dodávku serverům a síťovým prvkům a nějaké podmnožině pracovních stanic. K úplnému pokrytí dodávky proudu do celého objektu společnosti včetně obchodních jednotek by byla potřeba investice vyšší.

Poruchy hardwaru

Pokud přihlédneme ke skutečnosti, že veškerá klíčová data by měla být centrálně uložena na serverech, pak je důležité obrátit pozornost právě tímto směrem. Jestliže je tedy v zájmu ochránit data, jsou nenákladným řešením disková pole umožňující pomocí parity dopočítat data ztracená kvůli selhání některého z disků. Pravděpodobnost paralelního selhání více disků najednou rapidně klesá. Pro potřeby pořizování komplexních záloh by bylo potřeba zakoupit páskové mechaniky, a to z důvodu snadné manipulace s nimi a snadné možnosti přenosu záloh na bezpečné místo mimo budovu pro případ požáru. Taková investice už začíná dosahovat řádově desetitisíců, avšak nepřesáhne v případě 800GB verze nekomprimovaně 100.000 Kč. S přihlédnutím ke skutečnosti, že každá společnost disponuje svými klíčovými

daty a veškerým know-how společnosti, je tato investice určitě namístě a může předejít škodám, které by mohly dosáhnout mnohem vyšších částek.

Počítačový virus

Jak již bylo zmíněno, ve společnosti FAOC nemají s viry větší problémy. Bylo také zjištěno, že spolu s navrženou bezpečnostní politikou je zabezpečení proti virovým nákazám dostatečné. Jelikož se problematika počítačových virů zároveň týká i pořizování pravidelných záloh, byla aktuální situace ve firmě prohlášena za uspokojivou. Je ovšem třeba prodloužit délku historie záloh, aby bylo možno efektivně snížit pravděpodobnost situace, kdy všechny pořízené zálohy jsou také infikované a tím pádem i znehodnocené pro potřeby obnovy. Tím dochází k potvrzení argumentu pro pořízení páskové mechaniky.

Chyby v programovém vybavení

Jelikož se společnost FAOC nezabývá vývojem softwarových aplikací a tedy veškeré programové vybavení, které potřebuje ke své činnosti, je zakoupeno, je tu hrozba pouze z této strany. Jestliže se tedy bude software pořizovat od renomovaných výrobců s kvalitní podporou a operační systémy všech počítačů budou řádně aktualizovány, snižuje se významně pravděpodobnost chyby způsobené softwarem. V případě nutnosti práce s obzvláště kritickými aplikacemi se také doporučuje řádné testování před ostrým nasazením do provozu.

4.3 Rekapitulace závěrů

Velké nedostatky jsou v organizačním zabezpečení činnosti IS ve společnosti. Není vypracována realistická bezpečnostní politika informačního systému. Rovněž je nutné přepracovat a doplnit stávající bezpečnostní dokumentaci pro uživatele. Plán obnovy IT zdrojů musí být rovněž vypracován jako samostatný dokument a musí být doplněn o konkrétní obnovovací procedury. Neexistuje také systém klasifikace dat.

Oblast zajištění zodpovědnosti za informace v IS je nedostatečná a je nutno urychleně vypracovat postupy pro přidělení odpovědnosti za informace, přidělení pouze nezbytně nutných práv k objektům dle stupně klasifikace atd. Dále je nutno vypracovat dělení zodpovědnosti za problematiku bezpečnosti informací v celé společnosti a v IS definováním vlastníků informací. Ve vrcholovém managementu musí být definován pracovník zodpovědný

za bezpečnost IS. Správce a jeho zodpovědnosti musí být zálohovány druhou pověřenou osobou, která bude vykonávat funkci bezpečnostního správce.

Případné náklady na snížení rizik budou shrnuty v následující tabulce.

Riziko	Investice	Důvod investice
Výpadky proudu	50 000 Kč – 100 000 Kč	Dieselový agregát s možností automatického elektrického spuštění z vlastního akumulátoru
Poruchy hardwaru	100 000 Kč	Pásková mechanika 800GB
Počítačový virus	0 Kč	Není potřeba investice
Chyby v programovém vybavení	0 Kč	Není potřeba investice

Z tabulky lze vyčíst, že případná výše investic na snížení rizik by mohla být vyčíslena až na 200 000 Kč.

5 Závěr

V dnešní době, kdy platí, že informace mají cenu zlata, neexistuje organizace (ať už se jedná o komerční subjekt nebo orgán veřejné správy), která by nějakými důležitými informacemi nedisponovala. Mohou to být informace z oblasti technického know-how, obchodní informace nebo jen osobní údaje zaměstnanců. Jedno však mají společné – je nutné je chránit. Není těžké si představit, co se může stát, pokud důležité informace (např. databáze klientů) budou nenávratně zničeny, nebo bude originální výrobní postup zaměstnancem vyzrazen konkurenci. Proto právě bezpečnostní audity mají přispět k zajištění takové ochrany.

Je důležité si uvědomit, že ačkoliv zajištění bezpečnosti informací představuje vynaložení určitých nákladů, nejedná se o investici, která žádný přímý užitek nepřináší a pouze zatěžuje rozpočet. Ve skutečnosti lze přínos bezpečnosti informací ocenit právě výší škod, které by mohly nastat, pokud bychom bezpečnost informací neřešili. V kapitole, která se zabývá návrhy na inovace bezpečnosti, byly takovéto výše nákladů odhadnuty.

Při bezpečnostním auditu byla odhalena rizika a zhodnocena protiopatření, která by měla firma přijmout. Vzhledem k aktuálním možnostem společnosti však některá z nich není možné zcela aplikovat, nicméně vedení je o problémech informováno. Do budoucna se tedy o těchto problémech bude dále zvažovat. Během auditu se též ukázala míra informovanosti a zejména nedostatečná dokumentace stavu společnosti. Mimo to byl poprvé stanoven seznam aktiv, u kterého se ukázalo, jak zaměstnanci pohlíží na jejich důležitost.

V rámci snižování rizika byly u dvou ze čtyř bezpečnostních incidentů s nejzávažnějším dopadem zjištěny nedostatky, které se ovšem i přesto nedají označit za fatální. Díky auditu byly také odhaleny nevhodné postupy, které vedly k nedostatečnému povědomí o tak závažných věcech, jako je oprávnění přístupu k serverům, kdy přístupem do technologické místnosti management centra disponovali všichni zaměstnanci společnosti. Mimo úprav stávajících bezpečnostních opatření bylo mnou navrženo několik nových, jedním z takových opatření by mohlo být např. automatizovaná pravidelná kontrola serverů.

V návaznosti na mou práci by bylo dobré provádět audit pravidelně. Přitom by se měla dle dosažených výsledků formalizovat pravidla auditu a dále aktualizovat bezpečnostní politika. Pro zajištění optimálních výsledků by se mohly vyzkoušet také jiné auditovací nástroje.

V samotném závěru bych dodal, že v konečném důsledku zůstává vždy na dané společnosti, jak se staví za bezpečnost svých informací a do jaké míry považuje za důležité je chránit před již zmiňovanými hrozbami.

Seznam použité literatury

1. KOPÁČIK, Ivan. *Riadenia a audit v informačnej bezpečnosti.* 7. vyd. Bratislava: TATE International Slovakia, 2007. 322 s. ISBN 978-80-969747-0-2.

2. *Common Criteria* [online]. 2014, [cit. 2014-04-02]. Common Criteria Portal. Dostupné z: <http://www.commoncriteriaportal.org/cc/>
3. *Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT* [online]. 2001, [cit. 2014-03-25]. Český normalizační institut. Dostupné z: < http://csnonlinefirmy.unmz.cz/html_nahledy/36/61397/61397_nahled.htm>
4. *Informační technologie – Bezpečnostní techniky – Specifikace služeb TTP na podporu aplikace digitálních podpisů* [online]. 2004, [cit. 2014-03-13]. Český normalizační institut. Dostupné z: <http://www.normservis.cz/download/view/csn/36/69321/69321_nahled.htm>
5. *Informační technologie – Směrnice pro řízení bezpečnosti IT – Část 3: Techniky pro řízení bezpečnosti IT* [online]. 2009, [cit. 2014-03-20]. Jiří Řezníček. Dostupné z: <http://www.technicke-normy-csn.cz/369786-csn-iso-iec-tr-13335-3_4_58372.html>
6. *ISMS v malých a středních firmách* [online]. 2003, [cit. 2014-03-26]. Risk Analysis Consultants. Dostupné z: <http://www.rac.cz/rac/homepage.nsf/CZ/Download/$FILE/ISMS%20pro%20SME%20051129.pdf>
7. *ISO/IEC 27002:2013* [online]. 2014, [cit. 2014-04-05]. Risk Analysis Consultants. Dostupné z: <http://www.rac.cz/rac/homepage.nsf/CZ/27002>
8. *ISO/IEC 27003:2010* [online]. 2014, [cit. 2014-04-06]. Risk Analysis Consultants. Dostupné z: <http://www.rac.cz/rac/homepage.nsf/CZ/FFDAEF05EF6A74BBC125706100497FA0?OpenDocument>
9. *ISO/IEC 27004:2009* [online]. 2014, [cit. 2014-04-07]. Risk Analysis Consultants. Dostupné z: <http://www.rac.cz/rac/homepage.nsf/CZ/27004>
10. *ISO/IEC 27005:2011* [online]. 2014, [cit. 2014-04-07]. Risk Analysis Consultants. Dostupné z: <http://www.rac.cz/rac/homepage.nsf/CZ/27005>

11. *ISO/IEC 27035:2011* [online]. 2014, [cit. 2014-04-15]. Risk Analysis Consultants. Dostupné z: < http://www.rac.cz/rac/homepage.nsf/CZ/27035>
12. *PDCA cyklus* [online]. 2012, [cit. 2014-04-27]. Jiří Střelec. Dostupné z: <http://www.vlastnicesta.cz/metody/pdca-cyklus-1/>
13. *Průzkum stavu informační bezpečnosti* [online]. 2009, [cit. 2014-04-29]. TATE International s.r.o. Dostupné z: <http://www.tate.cz/cz/download/>
14. *TCSEC* [online]. 2014,[cit. 2014-03-05]. Dostupné z: <http://www.pocitacovysvet.ic.cz/Bezpecnostni%20normy/tcsec.html>
15. *Zákony pro lidi* [online]. 2014, [cit. 2014-04-26]. AION CS. Dostupné z: <http://www.zakonyprolidi.cz/>

Seznam zkratek a pojmů

BSI – British standard Institution

CC – Common Criteria

CCTA – Central Computer and Telecommunications Agency

CRAMM – CCTA Risk Analysis and Management Method

ČR – Česká republika

ČSN – Česká technická norma

DoD – Department of Defense

DRP – Disaster Recovery Planning

EAL – Evaluation Assurance Level

ESSID – Extended Service Set Identification

FAOC – Fashion Arena Outlet Centrum

GB – Gigabyte

HDD – Hard disk drive

HP – Hewlett-Packard

ICT – Information and communication technologies

IDS – Intrusion detection systems

IRH – Incident Response Handling

IS – Informační systém

ISMS – Information security management system

ISO/IEC – International Organization for Standardization/International Electrotechnical Commission

IT – Informační technologie

ITSEC – The Information Technology Security Evaluation Criteria

KVM – Kernel-based Virtual Machine

LAN – Local Arena Network

LTS – Long-term support

Mgr. – Manager

MS – Microsoft

NAS – Network Attached Storage

NCSC – National Computer Security Center

NSA – National Security Agency

PC – Personal computer

PDCA – Plan, Do, Check, Action cyklus

PP – protection Profile

PSIB – Průzkum stavu informační bezpečnosti

RAID – Redundant array of independent disks

RAM – Random-access memory

SARs – Security Assurance Requirements

SFRs – Security Functional Requirements

ST – Security Target

TCB – Trusted Computing Base

TCSEC – Trusted Computer System Evaluation Criteria

TOE – Target Of Evaluation

TTP – Time-Triggered Protocol

WAN – World Area Network

Wi-fi – Wireless Fidelity

WPA – Wi-Fi Protected Access

Prohlašuji, že

- jsem byl seznámen s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, diplomovou práci užít (§ 35 odst. 3);
- souhlasím s tím, že diplomová práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího diplomové práce. Souhlasím s tím, že bibliografické údaje o diplomové práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, diplomovou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

Ve Veselí nad Moravou dne ……

……
jméno a příjmení studenta